ESET
Remote Administrator 4
Installations- und Benutzerhandbuch

ESET Remote Administrator 4

Copyright © 2010 **ESET, spol. s r.o.**
ESET Remote Administrator 4 wurde entwickelt von ESET, spol. s r.o.
Nähere Informationen finden Sie unter www.eset.com.
Alle Rechte vorbehalten. Ohne schriftliche Genehmigung des Verfassers darf diese Dokumentation weder ganz noch auszugsweise vervielfältigt, in einem Abrufsystem gespeichert oder übertragen werden. Dies gilt unabhängig von der verwendeten Form und dem technischen Verfahren (elektronisch, mechanisch, Fotokopie, Scannen, sonstige Aufzeichnung usw.).
ESET, spol. s r.o. behält sich das Recht vor, ohne gesonderte Ankündigung Änderungen an der beschriebenen Anwendungssoftware vorzunehmen.

Kundenservice weltweit: www.eset.eu/support
Kundenservice Nordamerika: www.eset.com/support

Versionsstand 14. 9. 2010

Inhalt

1. Einführung 5

1.1 Neuerungen 5

1.2 Programmarchitektur 7

2. Installation von ERA Server und ERA Console 8

2.1 Anforderungen 8

2.1.1 Softwareanforderungen 8

2.1.2 Leistungsanforderungen 8

2.1.3 Verwendete Ports 10

2.2 Installationsanleitung 10

2.2.1 Überblick zur Netzwerkumgebung 10

2.2.2 Vor der Installation 11

2.2.3 Installation 12

2.2.3.1 Installation von ERA Server 12

2.2.3.1.1 Cluster-Installation 13

2.2.3.2 Installation von ERA Console 13

2.2.3.3 Update-Mirror 13

2.2.3.4 Von ERA Server unterstützte Datenbanktypen 14

2.2.3.4.1 Grundvoraussetzungen 14

2.2.3.4.2 Einrichten der Datenbankverbindung 15

2.2.3.4.3 Installation über eine vorhandene Datenbank 16

2.3 Szenario - Installation in einer großen Unternehmensumgebung 16

2.3.1 Überblick zur Netzwerkumgebung 16

2.3.2 Installation 17

2.3.2.1 Installation in der Zentrale 17

2.3.2.2 Zweigniederlassung: Installation von ERA Server 17

2.3.2.3 Zweigniederlassung: Installation des HTTP-Mirror-Servers 17

2.3.2.4 Zweigniederlassung: Remoteinstallation auf den Clients 17

2.3.3 Weitere Voraussetzungen für große Unternehmensumgebungen 18

3. Die Arbeit mit ERAC 19

3.1 Verbindungsaufbau mit ERAS 19

3.2 ERAC - Hauptfenster 20

3.3 Filtern von Informationen 21

3.3.1 Filter 21

3.3.2 Kontextmenü 22

3.3.3 Anzeigemodus 23

3.4 Registerkarten in ERAC 23

3.4.1 Allgemeiner Überblick zu Registerkarten und Clients 23

3.4.2 Inhalt der Registerkarten bei Replikation 24

3.4.3 Clients (Registerkarte) 25

3.4.4 Bedrohungen (Registerkarte) 27

3.4.5 Firewall (Registerkarte) 28

3.4.6 Ereignisse (Registerkarte) 28

3.4.7 Scans (Registerkarte) 28

3.4.8 Mobilgeräte (Registerkarte) 29

3.4.9 Quarantäne (Registerkarte) 29

3.4.10 Tasks (Registerkarte) 29

3.4.11 Berichte (Registerkarte) 30

3.4.12 Remoteinstallation (Registerkarte) 30

3.5 Konfiguration von ERA Console 30

3.5.1 Verbindung (Registerkarte) 30

3.5.2 Spalten - Anzeigen/Ausblenden (Registerkarte) 30

3.5.3 Farben (Registerkarte) 30

3.5.4 Pfade (Registerkarte) 30

3.5.5 Datum/Uhrzeit (Registerkarte) 30

3.5.6 Sonstige Einstellungen (Registerkarte) 31

3.6 Anzeigemodi 31

3.7 ESET Configuration Editor 32

3.7.1 Arbeiten mit mehreren Konfigurationsebenen 33

3.7.2 Wesentliche Konfigurationseinträge 34

4. Installation von ESET Clientlösungen 36

4.1 Direkte Installation 36

4.2 Remoteinstallation 36

4.2.1 Anforderungen 39

4.2.2 Konfigurieren der Umgebung für die Remoteinstallation 39

4.2.3 Push-Remoteinstallation 40

4.2.4 Remoteinstallation per Anmeldeskript/E-Mail 43

4.2.5 Benutzerdefinierte Remoteinstallation 45

4.2.6 Upgrade 46

4.2.7 Vermeiden wiederholter Installationen 46

4.3 Installation in einer großen Unternehmensumgebung 47

5. Verwalten der Clientcomputer 48

5.1 Tasks 48

5.1.1 Konfigurations-Task 49

5.1.2 Task "On-Demand-Scan" 49

5.1.3 Task "Update starten" 50

5.1.4 SysInspector-Skript-Task 50

5.1.5 Task "Aus Quarantäne wiederherstellen/löschen" 51

5.1.6 Task "Sicherheits-Auditlog erzeugen" 51

5.1.7 Task "Hinweis anzeigen" 51

5.1.8 Interaktiver Task 52

5.2 Gruppen-Manager 53

5.2.1 Statische Gruppen 53

5.2.2 Parametrische Gruppen 54

5.2.3 Active Directory-Synchronisierung 54

5.3 Policies 55

5.3.1 Grundsätze und Funktionsweise 55

5.3.2 Erstellen von Policies 55

5.3.3 Virtuelle Policies 56

5.3.4 Rolle und Zweck von Policies in der Policyhierarchie 57

5.3.5 Anzeigen von Policies 58

5.3.6 Importieren/Exportieren von Policies 58

5.3.7 Zuweisen von Policies zu Clients 58

5.3.7.1 Standardpolicy für primäre Clients 59

5.3.7.2 Manuelle Zuweisung 59

5.3.7.3 Policyregeln 59

5.3.8 Löschen von Policies 60

5.3.9 Erweiterte Einstellungen 61

5.3.10 Szenarien für die Durchsetzung von Policies 61

5.3.10.1 Nur Standalone-Server, Policies werden lokal definiert 61

5.3.10.2 Jeder Server wird einzeln administriert - Policies werden lokal verwaltet, aber die übergeordnete Standardpolicy wird vom übergeordneten Server geerbt....63
5.3.10.3 Vererbung von Policies durch einen übergeordneten Server....64
5.3.10.4 Zuweisung von Policies ausschließlich vom übergeordneten Server....65
5.3.10.5 Zuweisung über Policyregeln....65
5.3.10.6 Zuweisung an Gruppen....66
5.4 Notifikationen....66
5.4.1 Notifikations-Manager....67
5.4.1.1 Notifikationen per SNMP-Trap....72
5.4.2 Erstellen von Regeln....72
5.5 Ausführliche Informationen von Clients....73
5.6 Zentrale Quarantäne....74

6. Assistent zum Zusammenführen von Firewall-Regeln....75

7. Berichte....76

7.1 Beispielszenario für die Berichtfunktionen....78

8. Konfiguration von ESET Remote Administrator Server (ERAS)....79

8.1 Sicherheit....79
8.2 Serverwartung....79
8.3 Mirror-Server....80
8.3.1 Betrieb des Mirror-Servers....81
8.3.2 Update-Typen....82
8.3.3 Aktivieren und Konfigurieren des Mirror-Servers....82
8.3.4 Update-Mirror für Clients mit NOD32 Version 2.x....84
8.4 Replikation....84
8.5 Logging....86
8.6 Lizenzverwaltung....86
8.7 Erweiterte Einstellungen....87
8.8 Sonstige Einstellungen....88

9. ESET Remote Administrator Maintenance Tool....89

9.1 Angaben zum ERA Server....89
9.2 Aufgabentyp....89
9.2.1 ERA Server beenden....89
9.2.2 ERA Server starten....89
9.2.3 Datenbank übertragen....89
9.2.4 Datenbank sichern....90
9.2.5 Datenbank wiederherstellen....90
9.2.6 Tabellen löschen....90
9.2.7 Neuen Lizenzschlüssel installieren....90
9.2.8 Serverkonfiguration bearbeiten....90

10. Fehlerbehebung....91

10.1 Häufige Fragen (FAQ)....91
10.1.1 Probleme bei der Installation von ESET Remote Administrator auf Windows Server 2000/2003....91
10.1.2 Was bedeutet der GLE-Fehlercode?....91
10.2 Gängige Fehlercodes....91
10.2.1 Fehlermeldungen bei der Remoteinstallation von ESET Smart Security oder ESET NOD32 Antivirus über ESET Remote Administrator....91
10.2.2 Gängige Fehlercodes in era.log....92
10.3 Fehlerdiagnose bei Problemen mit ERAS....92

11. Tipps und Tricks....94

11.1 Taskplaner....94
11.2 Entfernen vorhandener Profile....96
11.3 Exportieren einer Clientkonfiguration ins XML-Format und Verwendungsmöglichkeiten....97
11.4 Kombinierter Update-Abruf für Notebooks....98
11.5 Installation von Produkten anderer Hersteller über ERA....99

12. ESET SysInspector....100

12.1 Einführung in ESET SysInspector....100
12.1.1 Starten von ESET SysInspector....100
12.2 Benutzeroberfläche und Bedienung....100
12.2.1 Menüs und Bedienelemente....101
12.2.2 Navigation in ESET SysInspector....102
12.2.3 Vergleichsfunktion....103
12.3 Befehlszeilenparameter....104
12.4 Dienste-Skript....104
12.4.1 Erstellen eines Dienste-Skripts....105
12.4.2 Aufbau des Dienste-Skripts....105
12.4.3 Ausführen von Dienste-Skripten....107
12.5 Tastaturbefehle....108
12.6 Systemanforderungen....109
12.7 Häufige Fragen (FAQ)....109

13. ESET SysRescue....111

13.1 Minimalanforderungen....111
13.2 Erstellen der Rettungs-CD....111
13.2.1 Ordner....112
13.2.2 ESET Antivirus....112
13.2.3 Erweiterte Einstellungen....112
13.2.4 Bootfähiges USB-Gerät....112
13.2.5 Brennen....113
13.3 Die Arbeit mit ESET SysRescue....113
13.3.1 Verwenden des ESET SysRescue-Mediums....113

1. Einführung

ESET Remote Administrator (ERA) ist eine Anwendung, mit der Sie ESET Produkte auf Arbeitsplatzrechnern und Servern in einer Netzwerkumgebung zentral administrieren können. Über die integrierte Task-Verwaltung von ESET Remote Administrator können Sie ESET Security-Lösungen komfortabel auf Remoterechnern installieren und schnell auf neue Probleme und Bedrohungen reagieren.

ESET Remote Administrator an sich bietet keinerlei zusätzlichen Schutz gegen Schadcode. Die eigentliche Schutzwirkung ist davon abhängig, dass auf den zu schützenden Arbeitsplatzrechnern bzw. Servern ein ESET Security-Produkt wie ESET NOD32 Antivirus oder ESET Smart Security installiert ist.
Zur Bereitstellung einer vollständigen ESET Security-Lösung sind die folgenden Schritte erforderlich:

- Installation von ERA Server (ERAS),
- Installation von ERA Console (ERAC),
- Installation auf den Clientcomputern (ESET NOD32 Antivirus, ESET Smart Security, Linux ESET Security-Client usw. ...)

HINWEIS: Ordner- und Dateipfade in diesem Dokument nehmen teilweise Bezug auf die folgenden Betriebssystem-Umgebungsvariablen:

%ProgramFiles% = in der Regel *C:\Programme*
%ALLUSERSPROFILE% = in der Regel *C:\Dokumente und Einstellungen\All Users*

1.1 Neuerungen

ESET Remote Administrator Version 4.0

- Unterstützung für ESET Smart Security/ESET NOD32 Antivirus 4.2
- Unterstützung für ESET Mail Security 4 for Microsoft Exchange Server
- Unterstützung für Desktop-Securitylösung unter Linux/Mac (ESET NOD32 Antivirus 4)
- Unterstützung für ESET Mobile Security

Neue Funktionen
- Remoteinstallation - überarbeitet
- Gruppenverwaltung - überarbeitet (statische Gruppen, parametrische Gruppen, verbesserte Synchronisierung mit Active Directory)
- Filter - verbesserte Funktionen (Richtlinienfilter, Filter für statische und parametrische Gruppen)
- Richtlinien - neue Parameter in Richtlinienregeln (Unterstützung für parametrische Gruppen), Import/Export von Richtlinien und Richtlinienregeln, Zusammenführen von Tasks, Assistent für Richtlinienregeln
- Benachrichtigungen - Unterstützung für parametrische Gruppen, einige Detailverbesserungen
- Zentrale Ansicht für die Quarantänedateien aller Clients (bei ESS/EAV ab Version 4)
- Berichte - Unterstützung für statische und parametrische Gruppen, neue Berichttypen (Mobilgeräte-Protokoll, Quarantäne, Firewall), neue Vorlagen
- Assistent zum Zusammenführen von Firewall-Regeln - im Trainingsmodus erlernte Regeln können so zusammengeführt werden
- Windows-/Domänen-Benutzerauthentifizierung in ERA Console
- Unterstützung für passive Windows-Cluster
- Unterstützt die Reinstallation älterer ERA-Versionen (3.x, 2.x, 1.x), vorhandene Daten können migriert werden
- Datenverkehr verschlüsselt mit AES-256

Neuer ESET Configuration Editor
- Unterstützung für neue ESET Security-Produkte
- Unterstützung für neue Funktionen von ERA Server
- Lizenzdateien im .zip-Format
- Möglichkeit zum Hinzufügen vordefinierter geplanter Tasks

ESET Remote Administrator Version 3.0

- Unterstützung für ESET Security-Produkte der Version 4.x
- Unterstützung für Linux-Lösungen

Neue Funktionen
- Verwaltung von Richtlinien
- Benachrichtigungs-Manager
- Lesezugriff auf Konsole
- Unterstützung für ESET SysInspector
- Bessere Skalierbarkeit bei der Datenübertragung
- Löschen replizierter Clients
- Zusammenführen von Lizenzschlüsseln/Lizenz-Manager
- Update-Mirror für ESET NOD32 Antivirus 2.x
- Neue Installation
- Neue Domänenfilter-Option unter „Nicht registrierte Computer"
- Komprimierung der Serverprotokolle (.zip-Format)
- Kleinere Probleme behoben, mehrere kleine Funktionen hinzugefügt
- Rettungs-CD

Interne Verbesserungen am Server
- Unterstützung für zusätzliche Datenbanktypen (MS Access, MS SQL Server, Oracle, MySQL)

Neuer ESET Configuration Editor
- Unterstützung für ESET Security-Produkte der Version 4.x

ESET Remote Administrator Version 2,0

- Unterstützung der neuen ESET Security-Produkte Version 3 (ESET Smart Security, ESET NOD32 Antivirus)
- Neue Protokolle (neue Spalten, Protokolle der ESET Personal Firewall)
- Neue Angaben zum Clientstatus für Clients der Version 3 (Schutzstatus, Schutzkomponenten, Systeminformationen)
- Tasks (Konfiguration, Update starten, On-Demand-Prüfung, interaktiver Task)
- Unterstützung für NOD32 Version 2 weiterhin vorhanden

Neue Funktionen
- Erweiterte Client-Identifikation (MAC-Adresse hinzugefügt)
- Erweiterte Möglichkeiten für die Remoteinstallation (Unterstützung für .msi-Pakete und benutzerdefinierte Pakete)
- Verbesserte Sicherheit (Verschlüsselung für alle neuen Clients des Servers möglich)
- Bessere Performance (Kommunikationsprotokoll mit Komprimierung)
- Weiterleitung von ThreatSense.Net-Daten über ERA Server
- Verbesserte Benutzeroberfläche (neue Grafiken, verbesserte Farbgebung für Statuswerte, erweiterte Filtermöglichkeiten, skalierbare Dialogfenster)
- Neue Berichtvorlage (ESS-Schema)
- Überwachung der Serverleistung (Daten, Abfragen)
- Update-Funktion in ERA Server (zur Aktualisierung wichtiger Informationen)
- Mirror-Funktion in ERA Server
- Erweiterte Möglichkeiten für die Remoteinstallation (Unterstützung für .msi-Pakete und benutzerdefinierte Pakete, Möglichkeit zur ERA-Remoteinstallation, Diagnose)

Interne Verbesserungen am Server
- Neue Replikation (Replikationspriorität, bessere Mehrstufen-Replikation)
- Neue Datenbankstruktur
- Neue Verzeichnisstruktur
- Verbesserungen bei der internen Sicherheit

Neuer ESET Configuration Editor
- Unterstützung für ESET Security-Produkte der Versionen 2 und 3
- Möglichkeit zur Konfiguration von ERA Server
- weitere kleinere neue Funktionen (Suche, benutzerdefinierte Einstellungen)

Neue Installationsroutine (MSI)
- Datenbankmigration aus Vorgängerversionen

Neue Dokumentation (Hilfe, Handbuch)

1.2 Programmarchitektur

Aus technischer Sicht besteht ESET Remote Administrator aus zwei separaten Komponenten: ERA Server (ERAS) und ERA Console (ERAC). Sie können ERA Server und ERA Console beliebig oft in Ihrem Netzwerk installieren, da die Lizenzvereinbarung keine Höchstzahl hierfür festlegt. Beschränkt wird lediglich die Anzahl der Clients, die Sie mit Ihrer ERA-Installation administrieren können.

ERA Server (ERAS)

Die Serverkomponente von ERA wird als Dienst ausgeführt, wofür eines der folgenden Betriebssysteme auf Microsoft Windows® NT-Basis erforderlich ist: NT4 SP6, 2000, XP, 2003, Vista, 7 oder 2008. Dieser Dienst dient hauptsächlich dazu, Daten von den Clients zu erfassen und ihnen Anforderungen und Befehle unterschiedlicher Art zu übermitteln. Solche Befehle (Konfigurations-Tasks, Remoteinstallationen usw.) werden in ERA Console (ERAC) erstellt. ERAS dient also als Schnittstelle zwischen ERAC und den Clientcomputern - hier werden alle Informationen erfasst, gepflegt und verarbeitet, bevor sie an die Clients oder ERAC übertragen werden.

ERA Console (ERAC)

ERAC ist die Clientkomponente von ERA und wird in der Regel auf einem Arbeitsplatzrechner installiert. Von diesem Rechner aus kann der Administrator dann die ESET Clientlösungen auf den einzelnen Clients verwalten. Die Verbindung von ERAC zur ERA-Serverkomponente läuft über den TCP-Port 2223. Hergestellt wird sie durch den Prozess console.exe, der in der Regel im folgenden Verzeichnis abgelegt ist:

%ProgramFiles%\ESET\ESET Remote Administrator\Console

Bei der Installation von ERAC müssen Sie eventuell den Namen eines ERAS eingeben. Beim Programmstart baut die Konsole dann automatisch eine Verbindung zu diesem Server auf. Selbstverständlich können Sie ERAC auch nach der Installation noch konfigurieren.

2. Installation von ERA Server und ERA Console

2.1 Anforderungen

ERAS wird als Dienst ausgeführt und benötigt daher ein Betriebssystem auf Microsoft Windows NT-Basis (NT4 SP6, 2000, XP, 2003, Vista, 7 oder 2008). Eine Serverversion von Microsoft Windows ist für den Betrieb von ERAS zwar nicht zwingend erforderlich; wir empfehlen jedoch, ERAS für einen möglichst reibungslosen Betrieb auf einem Server-Betriebssystem zu installieren. Der ERAS-Rechner sollte ständig online und für die folgenden Arten von Computern über das Netzwerk erreichbar sein:

- Clients (in der Regel Arbeitsplatzrechner)
- PC mit ERA Console
- Weitere Instanzen von ERAS (bei Replikation)

HINWEIS: ESET Remote Administrator 4 unterstützt uneingeschränkt eine Installation über ältere Versionen (3.x, 2.x, 1.x). Vorhandene Daten können migriert werden.

2.1.1 Softwareanforderungen

ERA Server

32-Bit-Betriebssysteme:	Windows NT4 SP6 oder höher
64-Bit-Betriebssysteme:	Windows XP oder höher
Datenbanken:	Microsoft Access (integriert) Microsoft SQL Server 2005 und höher MySQL 5.0 und höher Oracle 9i und höher
Windows Installer:	2.0

ERA Console

32-Bit-Betriebssysteme:	Windows 2000 oder höher
64-Bit-Betriebssysteme:	Windows XP oder höher
Windows Installer:	2.0
Internet Explorer:	Empfohlene Version: 6.0, Mindestvoraussetzung: 4.0 (eventuell werden dann einige Berichte nicht korrekt angezeigt)

2.1.2 Leistungsanforderungen

Die Serverleistung hängt von den folgenden Parametern ab:

1. **Verwendete Datenbank**
   - MS Access-Datenbank - Wird standardmäßig mit dem Server installiert. Diese Lösung empfiehlt sich zur Verwaltung von maximal einigen Hundert Clients. Allerdings gibt es für die Datenbank eine Größenbeschränkung von 2 GB. Daher müssen Sie alte Daten regelmäßig entfernen, indem Sie die Server-Bereinigung aktivieren und ein entsprechendes Intervall festlegen (unter **Extras** > **Serveroptionen** > **Serverwartung**).
   - Andere Datenbanken (MySQL, Microsoft SQL Server, Oracle) müssen zwar separat installiert werden, ermöglichen aber eventuell eine bessere Serverleistung. Achten Sie in diesem Fall unbedingt darauf, passende Hardware zu verwenden (insbesondere bei einer Oracle-Datenbank). Richten Sie sich hierfür nach den technischen Empfehlungen des Herstellers.
   - Bei einer Oracle-Datenbank müssen Sie die Cursor-Anzahl höher als den Wert **Maximale Anzahl aktiver Verbindungen** setzen (unter **Extras** > **Serveroptionen** > **Erweitert** > **Erweiterte Einstellungen bearbeiten** > **Erweitert**, standardmäßig 500). Um die erforderliche Cursor-Anzahl zu ermitteln, müssen Sie auch die Anzahl der untergeordneten Server (falls eine Replikation stattfindet) sowie Cursors von anderen Anwendungen mit Datenbankzugriff berücksichtigen.
   - In der Regel lässt sich mit einer externen Datenbank (d. h. die Datenbank ist auf einem anderen physischen System installiert) eine höhere Serverleistung erzielen.

2. **Intervall der Clientverbindungen**
   - Das Intervall für Clientverbindungen ist ab ESET Smart Security / ESET NOD32 Antivirus 4.2 standardmäßig auf 10 Minuten eingestellt. Wenn der Clientstatus in längeren oder kürzeren Zeitabständen aktualisiert werden soll,

können Sie diese Einstellung entsprechend ändern. Bedenken Sie dabei jedoch, dass die Serverleistung bei kürzeren Verbindungsintervallen abnimmt.

3. **Durchschnittliche Anzahl gemeldeter Ereignisse pro verbundenem Client**
   - Alle vom Client an den Server übertragenen Informationen werden unter dem dazugehörigen Ereignis aufgeführt (z. B. Bedrohungs-Log, Ereignis-Log, Scan-Log, Konfigurationsänderung). Dieser Parameter lässt sich zwar nicht direkt steuern, aber über damit zusammenhängende Einstellungen beeinflussen. So können Sie beispielsweise in der Serverkonfiguration (unter **Extras** > **Serveroptionen** > **Serverwartung**) festlegen, wie viele Log-Daten der Server maximal entgegennehmen soll (sowohl von direkt verbundenen als auch von replizierten Clients). Im Normalbetrieb können Sie von einem langfristigen Mittelwert von einem Ereignis alle vier Stunden pro Client ausgehen.

4. **Verwendete Hardware und Betriebssystem**
   - Es wird dringend empfohlen, die Mindest-Hardwareanforderungen für das Betriebssystem Ihres Servers einzuhalten und zusätzlich zu berücksichtigen, wie viele Clients bedient werden sollen.

Überlastung
Wenn ein Server überlastet ist (Beispiel: 20.000 Clients bauen alle 10 Minuten eine Verbindung zu einem Server auf, der nur 10.000 Clients bedienen kann), werden einige der Clientverbindungen übersprungen. Im obigen Beispiel würde durchschnittlich nur jede zweite Clientverbindung bedient (so, als ob das Verbindungsintervall nicht auf 10, sondern auf 20 Minuten eingestellt wäre). Für jede abgewiesene Verbindung wird eine entsprechende Meldung protokolliert: "*<SERVERMGR_WARNING> ServerThread: Maximale Anzahl von Threads für aktive Verbindungen erreicht (500), Verbindung wird vom Server abgewiesen*". Auch bei einer nur zeitweisen Überlastung des Servers kann es vorkommen, dass Verbindungen abgewiesen werden.
Sie können in den erweiterten Servereinstellungen unter **Maximale Anzahl aktiver Verbindungen** einen anderen Wert als den Standardwert 500 einstellen. Dies empfiehlt sich jedoch nur in Ausnahmefällen zur gezielten Behebung von Problemen. Bei einem sehr großzügig ausgelegten System mit entsprechender Datenbankleistung können Sie über diese Einstellung die Gesamtleistung des Servers anpassen.

Datenverkehr im Netzwerk
Im Normalbetrieb eines Servers kann man als Rechengrundlage davon ausgehen, dass ein Client, der alle 10 Minuten eine Verbindung aufbaut, 0,04 Ereignisse pro Verbindung meldet (ein Ereignis alle vier Stunden). Hierfür fallen etwa 2 KB Datenverkehr pro Verbindung an.
Falls nun ein Virus ausbricht und ein Client bei jeder Verbindung sieben Ereignisse meldet, kann das Datenaufkommen pro Verbindung auf bis zu 240 KB steigen. Falls die Daten (wie standardmäßig aktiviert) komprimiert werden, reduziert sich das Datenvolumen um gut 50 % auf etwa 120 KB pro Verbindung.
Dabei wurden bis jetzt nur direkte Clientverbindungen berücksichtigt, keine replizierten Verbindungen. Die Replikation findet in deutlich längeren Zeitabständen statt und dient zur Übertragung neuer Ereignisse von untergeordneten Servern. Welche Ereignisse in welchem Umfang automatisch repliziert werden, können Sie in den erweiterten Servereinstellungen festlegen (**Extras** > **Serveroptionen** > **Erweitert** > **Erweiterte Einstellungen bearbeiten** > **Replikation**). Im Bereich „Serverwartung" können Sie außerdem konfigurieren, in welchem Umfang der übergeordnete Server Logs entgegennimmt. Diese Einstellung gilt sowohl für direkt verbundene als auch für replizierte Clients.

Speicherplatzbedarf
Eine Erstinstallation des Produkts mit einer MS Access-Datenbank benötigt bis zu 60 MB Speicherplatz auf der Festplatte.
Zusätzlicher Speicherplatz wird hauptsächlich für Clientereignisse benötigt, die in der Datenbank sowie in einem Speicher auf dem Datenträger abgelegt werden (Standardverzeichnis: *C:\Dokumente und Einstellung\All Users\Anwendungsdaten\Eset\ESET Remote Administrator\Server*). Für den Betrieb von ERA müssen mindestens 5 % des Datenträgers noch frei sein. Fällt der verfügbare Speicherplatz unter diesen Grenzwert, nimmt der Server bestimmte Clientereignisse nicht mehr entgegen. Die betreffende Einstellung finden Sie unter **Extras** > **Serveroptionen** > **Erweitert** > **Erweiterte Einstellungen bearbeiten** > **Erweitert** > **Maximal ... Prozent der Festplatte belegen**. Wenn die Standardeinstellungen für die Server-Bereinigung aktiviert sind (d. h. Ereignisse, die älter als drei Monate sind, werden gelöscht), sind im Normalbetrieb etwa 10 GB freier Speicherplatz pro 1000 Clients erforderlich.

Fallbeispiel

Ein Server mit einer MS Access-Datenbank, dessen Clients alle fünf Minuten eine Verbindung aufbauen und pro Verbindung durchschnittlich sieben Ereignisse melden (Bedrohungs-, Ereignis-, Scan-Log, Konfigurationsänderungen usw.), kann zeitweise bis zu 3000 Clients bedienen. Dieses Szenario entspricht einer temporären Überlastungssituation, wie sie etwa bei der Ereignismeldung während eines Virenausbruchs auftritt.
Mit einer externen Datenbank und einem Client-Verbindungsintervall von 10 Minuten (sowie 0,02 Ereignissen pro Verbindung) kann der Server hingegen maximal 30.000 Clients bedienen. Bei diesem Szenario gehen wir davon aus,

dass die Datenbankleistung optimal ist und die Clients nur relativ wenig Ereignisse melden.
Mit einer MS Access-Datenbank und einem Client-Verbindungsintervall von 10 Minuten kann der Server im Normalbetrieb maximal 10.000 Clients bedienen.

2.1.3 Verwendete Ports

Die folgende Tabelle zeigt, welche Netzwerkverbindungen für die Arbeit mit ERAS je nach verwendeter Funktion erforderlich sind. Der Prozess EHttpSrv.exe überwacht den TCP-Port 2221 auf eingehende Verbindungen, der Prozess era.exe die TCP-Ports 2222, 2223, 2224 und 2846. Der restliche Datenverkehr läuft über nativ im Betriebssystem integrierte Prozesse (z. B. NetBIOS über TCP/IP).

Protokoll	Port	Beschreibung
TCP	2221 (ERAS ankommend)	Standardport für den HTTP-Server des integrierten Update-Mirrors von ERAS
TCP	2222 (ERAS ankommend)	Kommunikation zwischen Clients und ERAS
TCP	2223 (ERAS ankommend)	Kommunikation zwischen ERAC und ERAS

Um alle Programmfunktionen nutzen zu können, müssen die folgenden Ports geöffnet werden:

Protokoll	Port	Beschreibung
TCP	2224 (ERAS ankommend)	Kommunikation zwischen dem Agenten *einstaller.exe* und ERAS bei einer Remoteinstallation
TCP	2846 (ERAS ankommend)	ERAS-Replikation
TCP	139 (ERAS abgehend)	Kopieren des Agenten *einstaller.exe* von ERAS auf einen Client über die administrative Freigabe admin$
UDP	137 (ERAS abgehend)	Namensauflösung bei der Remoteinstallation
UDP	138 (ERAS abgehend)	Computersuche bei der Remoteinstallation
TCP	445 (ERAS abgehend)	Direkter Zugriff auf freigegebene Ressourcen über TCP/IP bei der Remoteinstallation (Alternative zu TCP 139)

Die vordefinierten Ports 2221, 2222, 2223, 2224 und 2846 können geändert werden, wenn sie bereits durch andere Anwendungen genutzt werden.

Um die ERA-Standardports zu ändern, klicken Sie auf **Extras** > **Serveroptionen**. Um einen anderen Port als 2221 zu verwenden, klicken Sie auf die Registerkarte **Updates** und ändern dort den Wert **Port für HTTP-Server**. Für die Funktionen mit den Standardports 2222, 2223, 2224 und 2846 können Sie im Bereich **Ports** der Registerkarte **Erweitert** andere Ports einrichten.

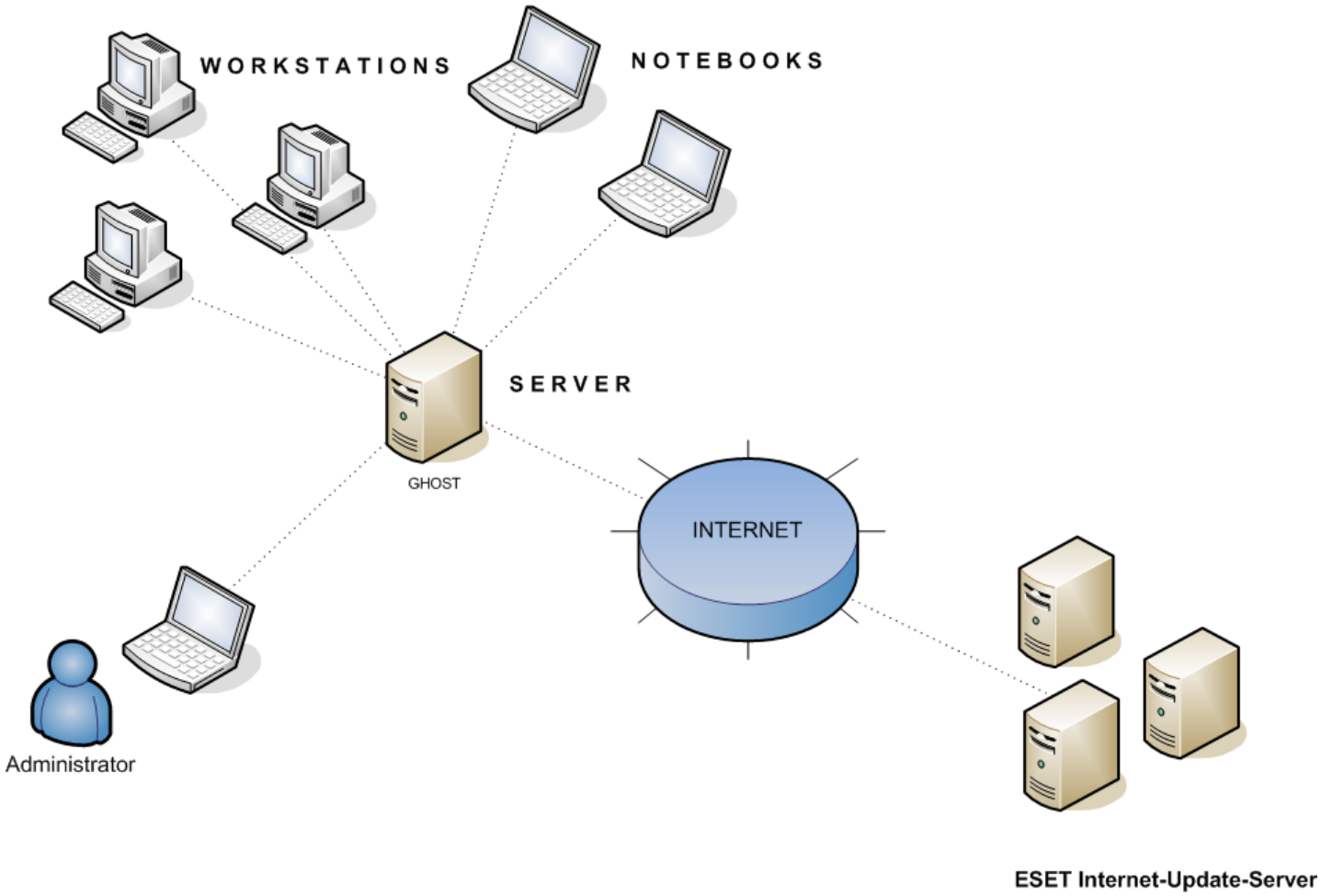
Die vordefinierten Ports 2222, 2223, 2224 und 2846 können Sie auch während der benutzerdefinierten Installation von ERAS ändern.

2.2 Installationsanleitung

2.2.1 Überblick zur Netzwerkumgebung

Bei einem typischen Firmennetz, das aus einem einzigen lokalen Netzwerk (LAN) besteht, empfiehlt sich die Installation eines ERAS sowie eines Mirror-Servers. Der Mirror-Server kann entweder in ERAS oder in ESET NOD32 Antivirus Business Edition / ESET Smart Security Business Edition aktiviert werden.

Für unser Beispiel nehmen wir an, dass es sich bei allen Clients um Desktops und Notebooks mit Microsoft Windows 2000/XP/Vista/7 handelt, die in einer Domäne vernetzt sind. Der Server GHOST ist rund um die Uhr online und kann unter einer Workstation-, Professional- oder Serverversion von Windows betrieben werden (ein Betrieb als Active Directory-Server ist nicht erforderlich). Außerdem nehmen wir an, dass die Notebooks bei der Installation der ESET Clientlösungen nicht im Netzwerk sind. Bei einem solchen Beispiel könnte die Netzwerkumgebung etwa wie folgt aussehen:



2.2.2 Vor der Installation

Vor der Installation sollten Sie die folgenden Installationspakete von der ESET-Website herunterladen:

ESET Remote Administrator-Komponenten:

ESET Remote Administrator - Server
ESET Remote Administrator - Console

ESET Clientlösungen:

ESET Smart Security 4.x
ESET Smart Security 3.x
ESET NOD32 Antivirus 4.x
ESET NOD32 Antivirus 3.x
ESET NOD32 Antivirus 2.7

Laden Sie nur diejenigen Clientlösungen herunter, die auf den Client-Arbeitsplatzrechnern tatsächlich verwendet werden sollen.

2.2.3 Installation

2.2.3.1 Installation von ERA Server

Installieren Sie ERAS auf dem Server GHOST (siehe dazu das Beispiel unter Überblick zur Netzwerkumgebung 10). Als Installationsart können Sie entweder **Typisch** oder **Benutzerdefiniert** auswählen.

Bei der Installationsart „Typisch" werden Sie gebeten, einen Lizenzschlüssel anzugeben. Hierbei handelt es sich um eine Datei mit der Erweiterung .lic oder .zip, die den Betrieb von ERAS über den in der Lizenz festgelegten Zeitraum ermöglicht. Im nächsten Schritt werden Sie gebeten, die Update-Einstellungen einzurichten (Benutzername, Passwort und Update-Server). Sie können diesen Schritt auch überspringen und die Update-Einstellungen später einrichten.

Bei der Installationsart „Benutzerdefiniert" bietet Ihnen das Installationsprogramm zusätzliche Konfigurationsmöglichkeiten. Die betreffenden Einstellungen können auch später noch über ERAC geändert werden; im Regelfall sollte dies jedoch nicht erforderlich sein. Die einzige Ausnahme ist der Servername, der mit dem DNS-Namen (Betriebssystem-Umgebungsvariable %COMPUTERNAME%) bzw. der IP-Adresse des Computers übereinstimmen muss. Hierbei handelt es sich um die wichtigste Angabe für Remoteinstallationen. Wenn dieser Name bei der Installation nicht angegeben wird, fügt das Installationsprogramm automatisch den Wert der Umgebungsvariablen %COMPUTERNAME% ein, was in den meisten Fällen ausreicht. Außerdem müssen Sie darauf achten, die richtige Datenbank zum Speichern der ERAS-Daten anzugeben. Nähere Informationen finden Sie im Kapitel Von ERA Server unterstützte Datenbanktypen 14.

Wichtig: In neueren Microsoft Windows-Versionen (Windows Vista, Windows Server 2008 und Windows 7) werden die Berechtigungen von lokalen Benutzerkonten durch entsprechende Sicherheitsrichtlinien eingeschränkt. Bestimmte Vorgänge im Netzwerk können über dieses Konto in manchen Fällen daher eventuell nicht ausgeführt werden. Wenn der ERA-Dienst auf Ihrem System unter einem lokalen Benutzerkonto ausgeführt wird, können bei bestimmten Netzwerkkonfigurationen Probleme bei der Push-Installation auftreten (z. B. bei einer Remoteinstallation aus einer Domäne in einer Arbeitsgruppe). Unter Windows Vista, Windows Server 2008 und Windows 7 empfiehlt es sich daher, den ERA-Dienst unter einem Konto mit ausreichenden Zugriffsrechten für das Netzwerk auszuführen. Das Benutzerkonto, unter dem ERA ausgeführt wird, können Sie in der Installationsart Benutzerdefiniert festlegen.

Hinweis: ERA Server unterstützt zwar uneingeschränkt Unicode, in manchen Situationen werden jedoch Zeichen in ANSI-Codierung umgewandelt oder umgekehrt (z. B. bei E-Mails und Computernamen). In diesen Fällen wird die im Betriebssystem festgelegten Standardsprache für Nicht-Unicode-Programme verwendet. Es empfiehlt sich, diese Einstellung an das Gebietsschema der Serverumgebung anzupassen, und zwar auch dann, wenn Sie die englische Version von ERA (d. h. keine übersetzte Sprachversion) verwenden. Die Einstellung finden Sie unter **Systemsteuerung** > **Regions- und Sprachoptionen** > Registerkarte **Erweitert**.

Die ERAS-Programmkomponenten werden standardmäßig im folgenden Ordner installiert:

%ProgramFiles%\ESET\ESET Remote Administrator\Server

Zusatzdaten wie Logs, Installationspakete, Konfigurationsdaten usw. werden im folgenden Ordner gespeichert:

%ALLUSERSPROFILE%\Anwendungsdaten \ESET\ESET Remote Administrator\Server

Der ERAS-Dienst wird nach der Installation automatisch gestartet. Die Aktivität des ERAS-Dienstes wird in der folgenden Datei protokolliert:

%ALLUSERSPROFILE%\Anwendungsdaten\ESET\ESET Remote Administrator\Server\logs\era.log

Installation über die Befehlszeile

ERAS kann auch über die Befehlszeile installiert werden. Dabei stehen Ihnen die folgenden Parameter zur Verfügung:

/q - Unbeaufsichtigte Installation. Es sind keinerlei Benutzereingriffe möglich. Es werden keine Dialogfenster angezeigt.
/qb - Es sind keine Benutzereingriffe möglich, der Verlauf der Installation wird jedoch über eine Fortschrittsleiste angezeigt.

Beispiel: *era_server_nt32_ENU.msi /qb*

Die Parameter der Befehlszeilen-Installation können durch eine XML-Konfigurationsdatei namens *cfg.xml* ergänzt

werden. Diese muss im gleichen Ordner wie die *.msi*-Installationsdatei für ERA liegen. Sie können diese Konfigurationsdatei im ESET Configuration Editor erstellen und auf diese Weise eine Reihe von ERA-Einstellungen konfigurieren. Nähere Informationen finden Sie im Kapitel ESET Configuration Editor 32.

2.2.3.1.1 Cluster-Installation

Bei einer benutzerdefinierten Installation können Sie auch eine **Cluster-Installation** durchführen. Hierbei müssen Sie den Pfad zu einem freigegebenen Cluster-Datenordner angeben, der von allen Knoten im Cluster aus zugänglich ist (d. h. alle Knoten müssen Lese- und Schreibrechte für den Ordner haben). Es kann sich dabei um einen Quorumdatenträger oder einen UNC-Pfad zu einem freigegebenen Ordner handeln. Bei einem freigegebenen Ordner müssen Sie in den Ordnereigenschaften die Freigabe für **Computer** aktivieren. Anschließend fügen Sie in den **Freigabeberechtigungen** den Namen des Cluster-Knotens mit Rechten für den Vollzugriff hinzu.
Sie müssen ERA Server separat auf jedem Cluster-Knoten installieren. Sofern nicht die integrierte MS-Access-Datenbank verwendet wird, achten Sie darauf, dass alle ERA Server-Knoten eine Verbindung zur selben Datenbank aufbauen. Achten Sie in den darauf folgenden Schritten außerdem darauf, als Servernamen den Namen des Cluster-Knotens anzugeben, auf dem ERA-installiert wird.

Wichtig: Sie müssen den ESET Remote Administrator Server-Dienst (ERA_SERVER) in der Konsole „Clusterverwaltung" als allgemeinen Clusterdienst konfigurieren.

Vor einer Deinstallation von ERA Server müssen Sie den Cluster-Knoten deaktivieren.

2.2.3.2 Installation von ERA Console

Installieren Sie ESET Remote Administrator Console auf dem PC bzw. Notebook des Administrators. Geben Sie am Ende der benutzerdefinierten Installation den Namen oder die IP-Adresse des ERA Servers an, zu dem ERAC beim Programmstart automatisch eine Verbindung aufbauen soll. In unserem Beispiel heißt der Serverrechner GHOST.

Starten Sie nach der Installation ERAC und überprüfen Sie die Verbindung zu ERAS. Standardmäßig ist zum Verbindungsaufbau mit einem ERA Server kein Passwort erforderlich (das Eingabefeld für das Passwort ist leer). Wir empfehlen jedoch dringend, ein Passwort einzurichten. Um ein Passwort für den Verbindungsaufbau zum ERA Server einzurichten, klicken Sie auf **Datei** > **Passwort ändern** und dann neben „Passwort für Konsole" auf **Ändern**.

Als Administrator können Sie unterschiedliche Passwörter für den Administratorzugriff und den Read-Only-Zugriff (Lesezugriff) einrichten. Im Read-Only-Zugriff können Benutzer die ERAS-Konfiguration nur einsehen, nicht jedoch bearbeiten.

2.2.3.3 Update-Mirror

Über ERA Console können Sie die Mirror-Funktion von ERA Server aktivieren, um einen eigenen Update-Server in Ihrem LAN einzurichten. Arbeitsplatzrechner im LAN können Updates dann von diesem Server abrufen. Auf diese Weise reduzieren Sie das Datenvolumen, das über Ihre Internetverbindung übertragen wird.

Gehen Sie wie folgt vor:

1) Bauen Sie in ERA Console eine Verbindung zu ERA Server auf, indem Sie auf **Datei** > **Verbinden** klicken.
2) Klicken Sie in ERA Console auf **Extras** > **Serveroptionen** und dann auf die Registerkarte **Updates**.
3) Wählen Sie in der Liste **Update-Server** die Option **Automatisch auswählen**. Belassen Sie das Update-Intervall auf 60 Minuten. Geben Sie unter **Update-Benutzername** den passenden Benutzernamen ein (EAV-****). Klicken Sie dann auf **Passwort festlegen** und geben Sie das Passwort ein, das Sie für den Benutzernamen erhalten haben (Sie können es auch kopieren und einfügen).
4) Aktivieren Sie die Option **Update-Mirror aktivieren**. Übernehmen Sie den Standardpfad für die Mirror-Dateien sowie die Porteinstellung für den HTTP-Server (2221). Belassen Sie die Einstellung **Authentifizierung** auf „Keine".
5) Klicken Sie auf die Registerkarte **Erweitert** und dann auf **Erweiterte Einstellungen bearbeiten**. Wählen Sie in der Einstellungshierarchie den Eintrag **ERA Server** > **Einstellungen** > **Update-Mirror** > **Mirror-Kopie der ausgewählten Programmkomponenten erstellen**. Klicken Sie im rechten Teil des Fensters auf **Bearbeiten** und wählen Sie die Programmkomponenten aus, die heruntergeladen werden sollen. Sie sollten die Komponenten für alle Sprachversionen auswählen, die im Netzwerk verwendet werden.
6) Klicken Sie auf der Registerkarte **Updates** auf **Update starten**, um die Mirror-Kopien zu erstellen.

Ausführlichere Informationen zu den Mirror-Konfigurationsoptionen finden Sie im Kapitel So aktivieren und konfigurieren Sie den Update-Mirror 82.

2.2.3.4 Von ERA Server unterstützte Datenbanktypen

Standardmäßig verwendet das Programm eine Microsoft Access-Datenbank (Jet-Engine). ERAS 4.0 unterstützt darüber hinaus die folgenden Datenbanken:

- Microsoft SQL Server 2005 und höher
- MySQL 5.0 und höher
- Oracle 9i und höher

Den Datenbanktyp können Sie bei einer benutzerdefinierten Installation von ERAS auswählen. Nach der Installation lässt sich der Datenbanktyp nicht mehr direkt aus ERA ändern. Hierzu können Sie jedoch das ERA Maintenance Tool 89 verwenden.

HINWEIS:
- Microsoft Access-Datenbanken werden unter Windows Server 2008 Core nicht unterstützt.
- Bei SQL Server Express ist die Datenbankgröße auf maximal 4 GB beschränkt.

2.2.3.4.1 Grundvoraussetzungen

Im ersten Schritt müssen Sie eine Datenbank auf einem Datenbankserver erstellen. Das ERAS-Installationsprogramm kann eine leere Datenbank erstellen. Diese erhält automatisch den Namen ESETRADB.

Standardmäßig erstellt das Installationsprogramm automatisch eine neue Datenbank. Wenn Sie die Datenbank von Hand erstellen möchten, wählen Sie die Option **Skript exportieren**. Stellen Sie dabei sicher, dass die Option **Automatisch Tabellen in der neuen Datenbank erstellen** deaktiviert ist.

Sortierungseinstellungen

Die Sortierung richtet sich nach den Standardeinstellungen der jeweiligen Datenbank. Der Server darf nicht zwischen Groß- und Kleinschreibung unterscheiden, d. h. die CI-Option (Case Insensitivity) muss aktiviert werden.

Gehen Sie dazu wie folgt vor:

- Microsoft SQL Server und MySQL: Richten Sie per COLLATE-Anweisung eine Sortierung mit aktiver CI-Option ein.
- Oracle: Richten Sie per NLS_SORT eine Sortierung mit aktiver CI-Option ein.
- MS Access: Keine weiteren Schritte erforderlich (CI-Option ist bereits aktiviert)

Zeichensatz

Insbesondere bei Clients mit unterschiedlichen Sprachversionen oder bei der Installation von ERA unter einem nicht-englischen Betriebssystem sollten Sie einen Unicode-Zeichensatz verwenden (empfohlene Codierung: UTF-8). Falls keine Replikation vorgesehen ist und alle Clients Verbindungen zum gleichen Server aufbauen, können Sie den Zeichensatz der zu installierenden ERA-Sprachumgebung verwenden.

MARS (Multiple Active Result Sets, mehrere aktive Resultsets)

Bei einer MS SQL-Datenbank ist für fehlerfreien Betrieb ein ODBC-Treiber mit MARS-Unterstützung erforderlich. Anderenfalls arbeitet der Server weniger effizient, und es wird die folgende Fehlermeldung ins Serverlog geschrieben:

Database connection problem. It is strongly recommended to use odbc driver that supports multiple active result sets (MARS). The server will continue to run but the database communication may be slower. See the documentation or contact ESET support for more information.

Bei anderen Datenbanken wird bei diesem Problem die folgende Meldung ins Serverlog geschrieben, und der Server wird beendet:

Database connection problem. Updating the odbc driver may help. You can also contact ESET support for more information.

Treiber ohne MARS-Unterstützung:
- SQLSRV32.DLL (2000.85.1117.00)
- SQLSRV32.DLL (6.0.6001.18000) - in Windows Vista und Windows Server 2008 integriert

Nativer Treiber mit MARS-Unterstützung:
- SQLNCLI.DLL (2005.90.1399.00)

2.2.3.4.2 Einrichten der Datenbankverbindung

Nachdem Sie eine neue Datenbank erstellt haben, müssen Sie die Verbindungsparameter für den Datenbankserver einrichten. Hierzu gibt es zwei Möglichkeiten:

1. Über einen DSN (Data Source Name, Datenquellenname)
   Zum manuellen Einrichten des DSN öffnen Sie den ODBC-Datenquellen-Administrator
   (Klicken Sie auf **Start > Ausführen** und geben Sie den Befehl *odbcad32.exe* ein.)

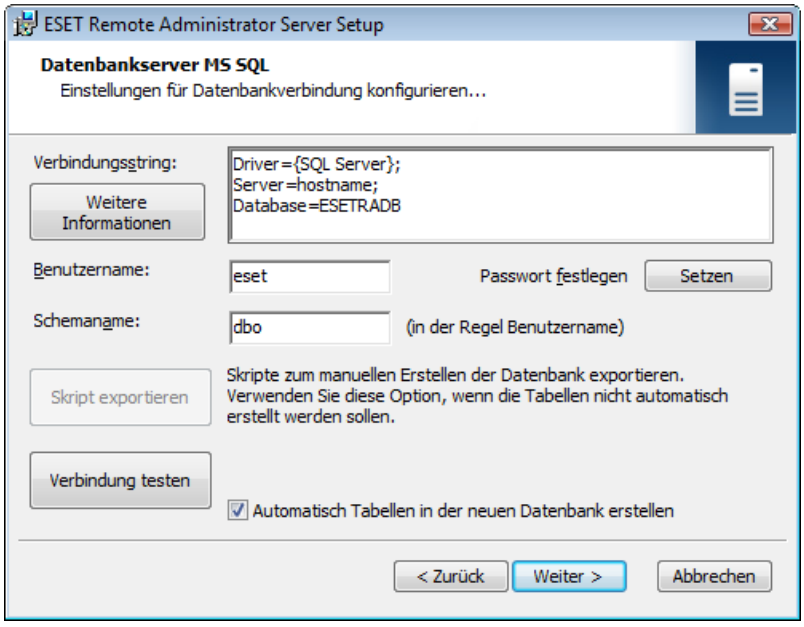
   Beispiel für eine Verbindung per DSN:
   DSN =ERASqlServer

   Wichtig: Für den ordnungsgemäßen Betrieb von ERA sollten Sie einen *System-DSN* verwenden.

   Für eine erfolgreiche Installation auf einem Microsoft SQL Server mit Windows-/Domänen-Authentifizierung müssen Sie einen Verbindungsstring im DSN-Format verwenden.

2. Direkt über einen vollständigen Verbindungsstring
   Hier müssen Sie alle erforderlichen Parameter direkt angeben: Treiber, Server sowie den Namen der Datenbank.

   Beispiel eines vollständigen Verbindungsstrings für Microsoft SQL Server:
   Driver ={SQL Server}; Server =Hostname; Database =ESETRADB



Beispiel eines vollständigen Verbindungsstrings für einen Oracle-Server:
Driver ={Oracle in instantclient10_1}; dbq =Hostname: 1521/ESETRADB

Beispiel eines vollständigen Verbindungsstrings für einen MySQL-Server:
Driver ={MySQL ODBC 3.51 Driver}; Server =Hostname; Database =ESETRADB

Legen Sie anschließend den **Benutzernamen** und das **Passwort** für die Verbindung fest (über die Schaltfläche **Festlegen**). Bei einer Oracle- oder Microsoft SQL Server-Datenbank müssen Sie außerdem einen **Schemanamen** angeben (bei SQL Server in der Regel identisch mit dem Benutzernamen).
Klicken Sie auf **Verbindung testen**, um die Verbindung zum Datenbankserver zu überprüfen.

Hinweis: Wir empfehlen, anstatt der Windows-/Domänen-Authentifizierung die interne Authentifizierung des Datenbankservers zu verwenden.

2.2.3.4.3 Installation über eine vorhandene Datenbank

Falls die Datenbank bereits Tabellen enthält, zeigt das Installationsprogramm eine entsprechende Meldung an. Um die vorhandenen Tabellen zu überschreiben, wählen Sie **Überschreiben** (***Warnung:*** Hiermit wird sowohl der Inhalt der Tabellen gelöscht als auch ihre Struktur überschrieben!). Wählen Sie **Überspringen**, um die vorhandenen Tabellen unverändert beizubehalten.

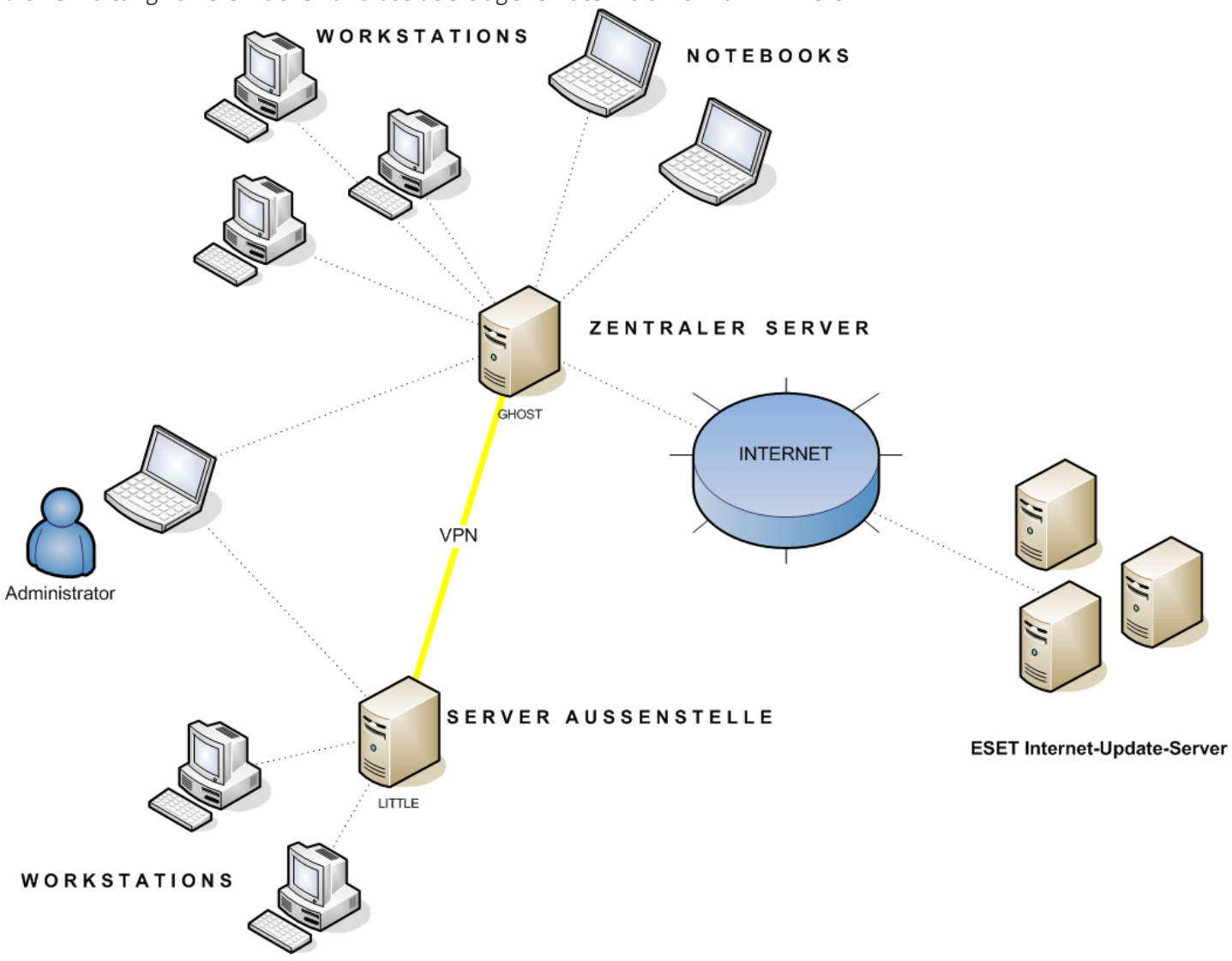
HINWEIS: Unter bestimmten Bedingungen kann die Option **Überspringen** zu Datenbankfehlern aufgrund von Inkonsistenzen führen. Dies gilt insbesondere dann, wenn Tabellen beschädigt oder mit der aktuellen Version inkompatibel sind.

Um die ERAS-Installation abzubrechen und die Datenbank manuell zu untersuchen, klicken Sie auf **Abbrechen**.

2.3 Szenario - Installation in einer großen Unternehmensumgebung

2.3.1 Überblick zur Netzwerkumgebung

Die folgende Abbildung zeigt eine Kopie der vorhergehenden Netzwerkumgebung mit einer zusätzlichen Zweigniederlassung, mehreren Clients und einem Server namens LITTLE. Nehmen wir an, zwischen der Zentrale und der Zweigniederlassung besteht nur eine langsame VPN-Verbindung. In einem solchen Szenario sollte der Mirror-Server auf dem Server LITTLE installiert werden. Außerdem werden wir einen zweiten ERA Server auf LITTLE installieren, um die Verwaltung zu vereinfachen und das übertragene Datenvolumen zu minimieren.

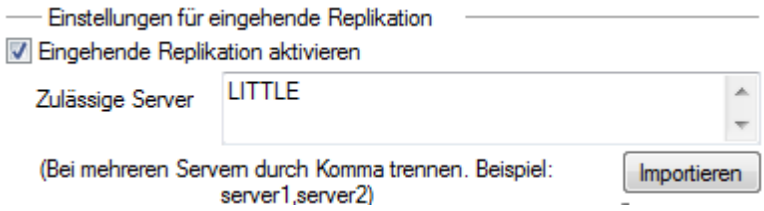


2.3.2 Installation

2.3.2.1 Installation in der Zentrale

Die Installation von ERAS, ERAC sowie der Client-Arbeitsplatzrechner läuft fast genauso ab wie im vorhergehenden Szenario. Der einzige Unterschied liegt in der Konfiguration des Master-ERAS (GHOST). Aktivieren Sie unter **Extras** > **Serveroptionen** > **Replikation** das Kontrollkästchen **Eingehende Replikation aktivieren** und tragen Sie den Namen des sekundären Servers im Feld **Zulässige Server** ein. In unserem Fall heißt der untergeordnete Server LITTLE.

Falls auf dem übergeordneten Server ein Passwort für die Replikation eingerichtet ist (**Extras** > **Serveroptionen** > **Sicherheit** > **Passwort für Replikation**), muss dieses in den Einstellungen für die ausgehende Replikation auf dem untergeordneten Server eingetragen werden.



2.3.2.2 Zweigniederlassung: Installation von ERA Server

Installieren Sie wie im vorhergehenden Beispiel den zweiten ERAS samt ERAC. Aktivieren und konfigurieren Sie auch hier die Replikationseinstellungen. Aktivieren Sie diesmal das Kontrollkästchen **Ausgehende Replikation aktivieren** (**Extras** > **Serveroptionen** > **Replikation**) und geben Sie den Master-ERAS an. Es empfiehlt sich, die IP-Adresse des Master-Servers zu verwenden, also in diesem Fall die IP-Adresse des Servers GHOST.

2.3.2.3 Zweigniederlassung: Installation des HTTP-Mirror-Servers

Die Konfiguration für die Installation des Mirror-Servers aus dem vorhergehenden Szenario kann auch hier verwendet werden. Die einzige Änderung betrifft die Einrichtung von Benutzername und Passwort.

Wie in der Abbildung im Kapitel Überblick zur Netzwerkumgebung 16 werden die Updates für die Zweigniederlassung nicht von den ESET-Update-Servern, sondern vom Server GHOST in der Zentrale heruntergeladen. Als Update-Quelle wird die folgende URL eingestellt:

http://ghost:2221 (oder http://IP-Adresse_von_GHOST:2221)

Standardmäßig muss kein Benutzername und Passwort angegeben werden, da der integrierte HTTP-Server keine Authentifizierung erfordert.

Nähere Informationen zur Konfiguration der Mirror-Funktion in ERAS finden Sie im Kapitel Mirror-Server 80.

2.3.2.4 Zweigniederlassung: Remoteinstallation auf den Clients

Auch hier kann wieder das bisherige Modell zum Einsatz kommen. Allerdings bietet es sich an, alle Arbeiten in ERAC über eine direkte Verbindung zum ERAS in der Zweigniederlassung auszuführen (in unserem Beispiel der Rechner LITTLE). So müssen die Installationspakete nicht über die langsamere VPN-Verbindung übertragen werden.

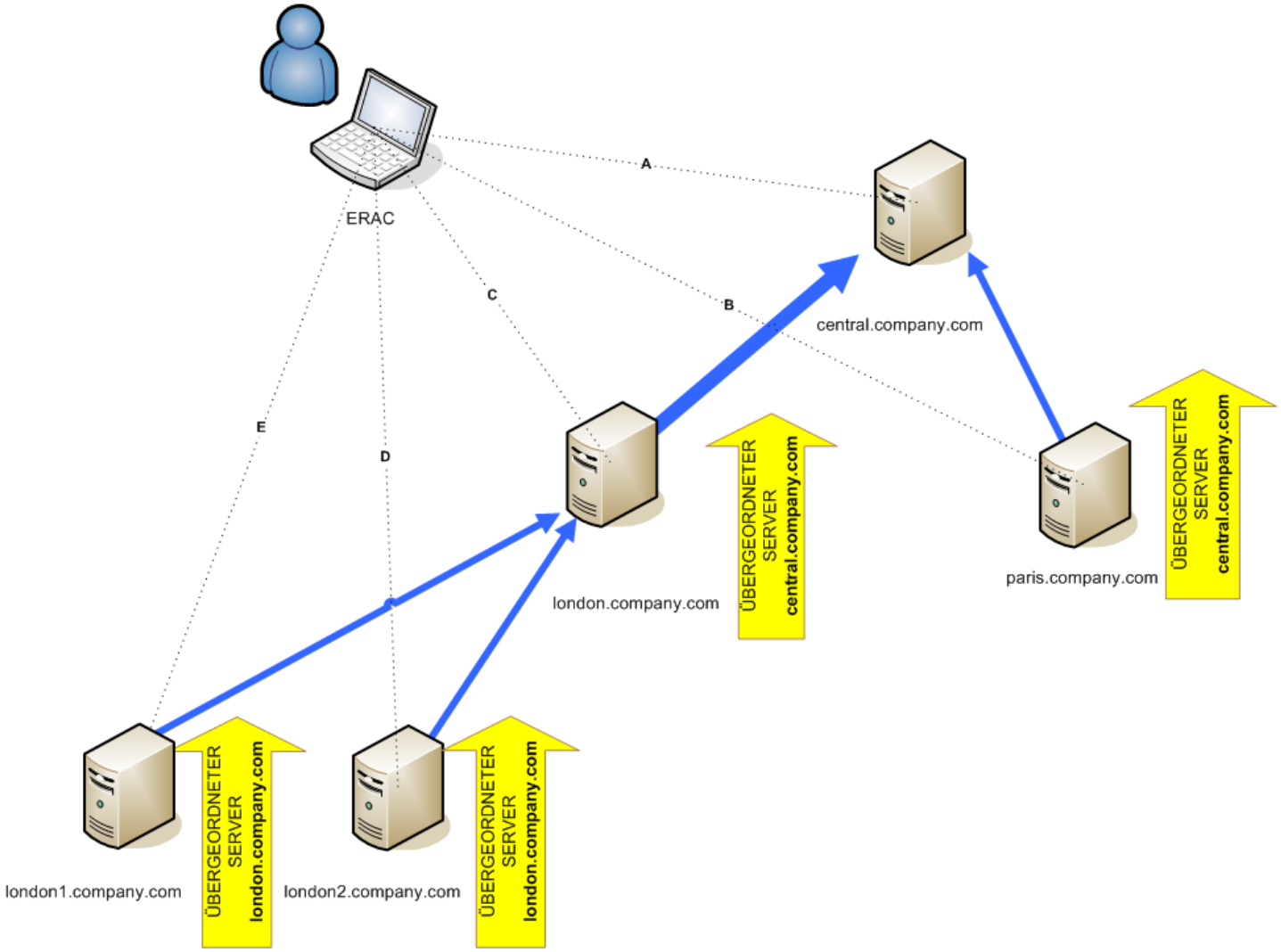
2.3.3 Weitere Voraussetzungen für große Unternehmensumgebungen

In größeren Netzwerken können mehrere ERA Server installiert werden, um eine bessere Zugänglichkeit der Server bei Remoteinstallationen auf Clientcomputern zu gewährleisten. Hierzu bietet ERAS die Möglichkeit zu einer *Replikation* (nähere Informationen siehe Kapitel Installation in der Zentrale 17 sowie Zweigniederlassung: Installation von ERA Server 17), bei der gespeicherte Daten an einen *übergeordneten ERAS* weitergeleitet werden. Die Replikation kann in ERAC konfiguriert werden.

Eine Replikation ist besonders bei Unternehmen mit mehreren Zweigniederlassungen oder entlegeneren Filialen sehr hilfreich. In unserem Beispiel würden Sie hierzu ERAS in jeder Zweigniederlassung installieren und jeweils eine Replikation auf einen zentralen ERAS einrichten. Der Vorteil einer solchen Konfiguration zeigt sich besonders deutlich bei privaten Netzwerken, die über eine (meist langsamere) VPN-Verbindung angebunden sind. Der Administrator muss hier lediglich auf den zentralen ERAS zugreifen (Verbindung A in der nachstehenden Abbildung). Ein VPN-Zugriff auf die einzelnen Zweigniederlassungen (Verbindungen B, C, D, E) ist überflüssig. Mithilfe der ERAS-Replikation wird der langsamere Kommunikationskanal auf diese Weise umgangen.

Bei der Konfiguration der Replikation kann der Administrator festlegen, welche Informationen automatisch in festen Zeitabständen an die übergeordneten Server übermittelt und welche Daten demgegenüber nur auf Abruf gesendet werden, wenn der Administrator eines übergeordneten Servers sie anfordert. Durch die Replikation wird ERA also nicht nur benutzerfreundlicher, es reduziert sich auch der Datenverkehr im Netzwerk.

Eine Replikation bietet darüber hinaus auch den Vorteil, dass sich mehrere Benutzer mit unterschiedlichen Berechtigungsstufen anmelden können. Der Administrator, der über die Konsole auf den ERAS london2.company.com zugreift (Verbindung E), kann nur diejenigen Clients verwalten, die mit london2.company.com verbunden sind. Der Administrator, der auf den zentralen Server central.company.com zugreift (Verbindung A), kann hingegen alle Clients sowohl in der Firmenzentrale als auch in den einzelnen Zweigniederlassungen verwalten.



3. Die Arbeit mit ERAC

3.1 Verbindungsaufbau mit ERAS

Auf die meisten Funktionen in ERAC können Sie erst zugreifen, nachdem Sie eine Verbindung zu ERAS aufgebaut haben. Vor dem Verbindungsaufbau definieren Sie den Server über seinen Hostnamen oder seine IP-Adresse:

Öffnen Sie ERAC, klicken Sie auf **Datei** > **Verbindungen bearbeiten** (oder **Extras** > **Konsolenoptionen**) und dann auf die Registerkarte **Verbindung**.

Klicken Sie auf **Hinzufügen/Entfernen**, um einen neuen ERA Server hinzuzufügen oder die vorhandenen Servereinträge zu bearbeiten. Wählen Sie in der Liste **Verbindung auswählen** den gewünschten Server aus. Klicken Sie dann auf **Verbinden**.

Weitere Optionen in diesem Fenster:

- **Beim Start der Konsole automatisch mit ausgewähltem Server verbinden**
  Wenn diese Option aktiviert ist, wird beim Start der Konsole automatisch eine Verbindung zum ausgewählten ERAS aufgebaut.
- **Meldung bei fehlgeschlagener Verbindung**
  Bewirkt, dass bei einem Kommunikationsfehler zwischen ERAC und ERAS eine entsprechende Meldung angezeigt wird.

Für die Authentifizierung stehen zwei Verfahren zur Verfügung:

ERA Server

Der Benutzer authentifiziert sich mit seinen ERAS-Anmeldedaten. Standardmäßig ist zum Verbindungsaufbau mit einem ERAS kein Passwort erforderlich. Wir empfehlen jedoch dringend, ein Passwort einzurichten. Um ein Passwort für den Verbindungsaufbau mit einem ERAS einzurichten, gehen Sie wie folgt vor:

Klicken Sie auf **Datei** > **Passwort ändern** (oder **Extras** > **Serveroptionen** > **Sicherheit**) und dann auf die Schaltfläche **Ändern** rechts neben **Passwort für Konsole**.

Beim Eingeben eines Passworts können Sie die Option **Passwort speichern** aktivieren. Bedenken Sie dabei aber bitte, dass dies ein Sicherheitsrisiko darstellen kann. Um alle gespeicherten Passwörter zu löschen, klicken Sie auf **Datei** > **Gespeicherte Passwörter löschen**.

Wählen Sie in der Liste **Zugriff** den Zugriffsmodus aus (**Administrator** oder **Nur Read-Only-Zugriff**), geben Sie Ihr Passwort ein und klicken Sie auf **OK**.

Windows/Domäne

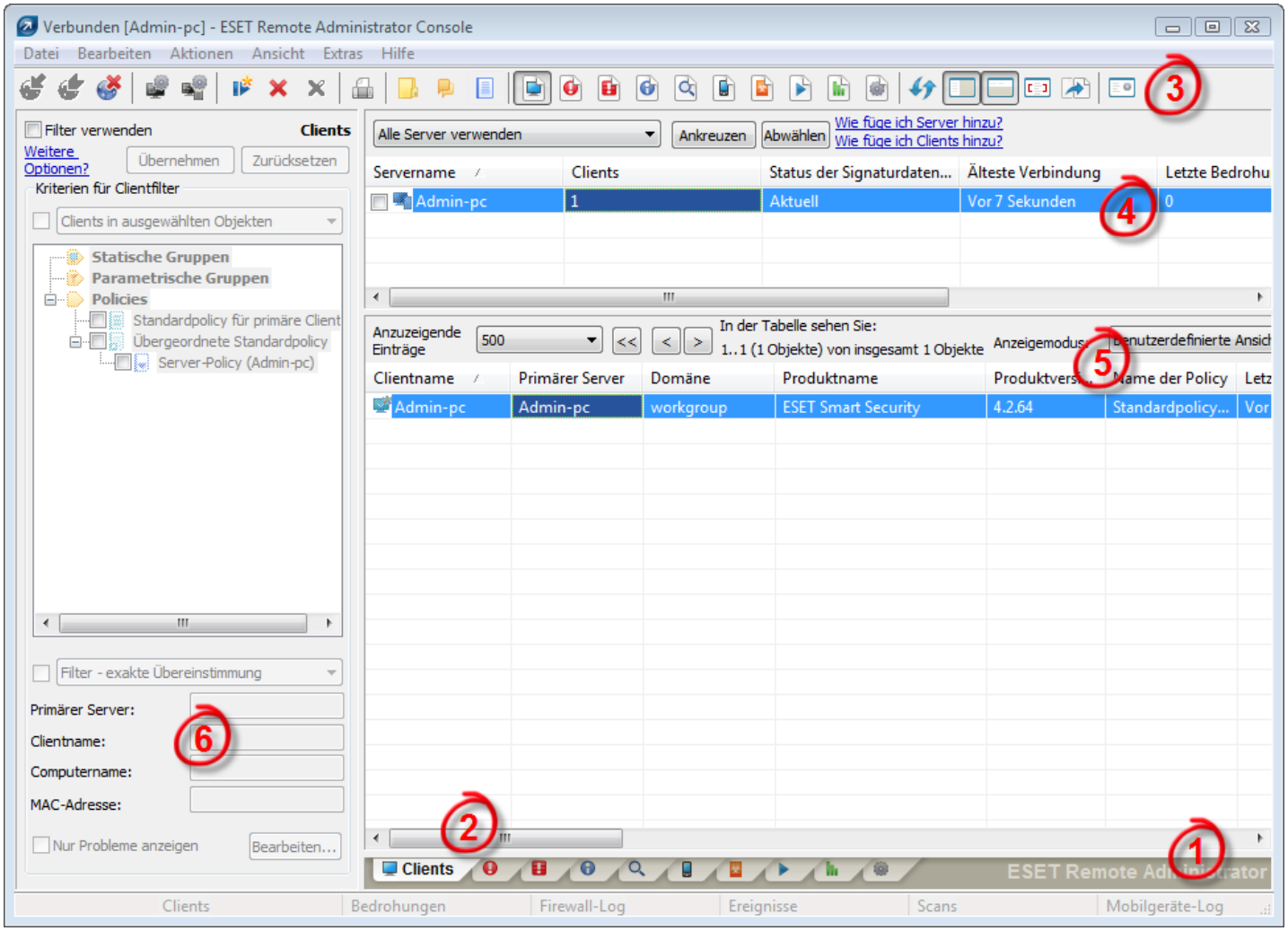
Der Benutzer authentifiziert sich mit seinen Windows- bzw. Domänen-Anmeldedaten. Damit die Windows-/Domänen-Authentifizierung korrekt funktioniert, muss ERAS unter einem Windows-/Domänenkonto mit ausreichenden Rechten installiert worden sein. Außerdem müssen Sie diese Funktion aktivieren. Verwenden Sie hierzu die folgenden Optionen unter **Extras** > **Serveroptionen** > Registerkarte **Erweitert** > **Erweiterte Einstellungen bearbeiten** > **ESET Remote Administrator** > **ERA Server** > **Einstellungen** > **Sicherheit**:

Windows-/Domänen-Authentifizierung zulassen - Aktiviert bzw. deaktiviert die Windows-/Domänen-Authentifizierung.
Administratorgruppen - Hier können Sie die Gruppen definieren, für die die Windows-/Domänen-Authentifizierung aktiviert werden soll.
Gruppen mit Read-Only-Zugriff - Hier können Sie die Gruppen definieren, die nur Lesezugriff (Read-Only-Zugriff) haben sollen.

Sobald die Verbindung zum Server steht, erscheint in der Titelleiste des Programms der Hinweis **Verbunden [Servername]**.
Stattdessen können Sie auch auf **Datei** > **Verbinden** klicken, um eine Verbindung zu ERAS aufzubauen.

HINWEIS: Der Datenverkehr zwischen ERAC und ERAS findet verschlüsselt statt (AES-256).

3.2 ERAC - Hauptfenster



Der aktuelle Status der Verbindung zwischen ERAC und ERAS wird in der Statusleiste angezeigt (1). Alle erforderlichen Daten von ERAS werden regelmäßig aktualisiert (standardmäßig jede Minute, Einstellung möglich unter **Extras** > **Konsolenoptionen**). Der Status der Aktualisierung wird ebenfalls in der Statusleiste angezeigt.

HINWEIS: Drücken Sie F5, um die angezeigten Daten von Hand zu aktualisieren.

Die angezeigten Daten sind nach der Reihenfolge ihrer Wichtigkeit in mehrere Registerkarten gegliedert (2). In den meisten Fällen können Sie die Daten durch Klicken auf einen Spaltenkopf (5) auf- oder absteigend sortieren. Per Drag&Drop können Sie die Reihenfolge der Anzeigespalten selbst verändern. Wenn viele Datensätze vorhanden sind, können Sie die Anzahl der angezeigten Einträge über die Liste **Anzuzeigende Einträge** einschränken und mit den Navigationsschaltflächen durch die Einträge blättern. Durch Auswahl eines **Ansichtsmodus** können Sie je nach Bedarf festlegen, welche Spalten angezeigt werden sollen (nähere Informationen siehe im Kapitel Filtern von Informationen 21).

Der Serverbereich (4) ist wichtig, wenn Sie ERA Server replizieren. Hier sehen Sie Überblicksinformationen zu der Konsole, mit der ERAS verbunden ist, sowie Angaben zu untergeordneten ERA Servern. Die Liste „Server" im Bereich 4 legt fest, woher die im Bereich 5 angezeigten Daten stammen.

- **Alle Server verwenden**
  Bewirkt, dass im Bereich (5) Daten von allen ERA Servern angezeigt werden.

- **Nur ausgewählte Server verwenden**
  Bewirkt, dass im Bereich (5) nur Daten von den ausgewählten ERA Servern angezeigt werden.

- **Ausgewählte Server nicht verwenden**
  Bewirkt, dass Daten von den ausgewählten ERA Servern nicht angezeigt werden.

Spalten im Bereich 4:

- **Servername**
  Name des Servers

- **Clients**
  Anzahl der Clients, die insgesamt mit dem ausgewählten ERAS verbunden sind, d. h. sich in dessen Datenbank befinden

- **Status der Signaturdatenbank**
  Version der Signaturdatenbank auf den Clients des ausgewählten ERAS

- **Älteste Verbindung**
  Zeitdauer seit der ältesten Verbindung zum Server

- **Letzte Bedrohungswarnungen**
  Gesamtanzahl der Virenwarnungen (siehe Attribut **Letzte Bedrohungswarnung** in Bereich 5)

- **Letzte Firewall-Warnungen**
  Gesamtanzahl der Firewall-Warnungen

- **Letzte Ereigniswarnungen**
  Gesamtanzahl der aktuellen Ereignisse (siehe Attribut **Letzte Ereigniswarnung** in Bereich 5)

Wenn keine Verbindung besteht, können Sie mit der rechten Maustaste auf einen Servereintrag im Serverbereich (4) klicken und **Mit diesem Server verbinden** wählen, um eine Verbindung zu diesem ERAS aufzubauen.

Bei aktivierter Replikation werden im Serverbereich (4) weitere Informationen angezeigt.

Die wesentlichen Funktionen von ERAC stehen über das Hauptmenü oder über die ERAC-Symbolleiste (3) zur Verfügung.

Nähere Informationen zum Bereich 6 (**Kriterien für Clientfilter**) finden Sie im Kapitel Filtern von Informationen 21.

3.3 Filtern von Informationen

ERAC bietet umfassende Werkzeuge und Funktionen zur komfortablen Administration von Clients und Ereignissen. Hierzu gehören auch leistungsstarke Filtermöglichkeiten, die besonders bei Systemen mit vielen Clients sehr hilfreich sind. Die angezeigten Informationen lassen sich damit unkompliziert gruppieren und verwalten. Zum Sortieren und Filtern von Informationen zu den verbundenen Clients stehen Ihnen in ERAC verschiedene Werkzeuge zur Verfügung.

3.3.1 Filter

Mithilfe von Filtern können Sie sich gezielt Informationen zu bestimmten Servern oder Client-Arbeitsplatzrechnern anzeigen lassen. Um die Filteroptionen anzuzeigen, klicken Sie im ERAC-Hauptmenü auf **Ansicht** > **Filterbereich anzeigen**.

Zum Anwenden eines Filters aktivieren Sie die Option **Filter verwenden** oben links im ERAC-Fenster. Sobald Sie die Filterkriterien ändern, werden die angezeigten Daten automatisch aktualisiert, es sei denn, Sie haben diese Funktion deaktiviert (**Extras** > **Konsolenoptionen** > Registerkarte **Sonstige Einstellungen**).

Definieren Sie im Bereich „Kriterien für Clientfilter" die Filterkriterien. Clients können mehreren Gruppen und Policies angehören. Die Zuordnung von Clients zu statischen oder parametrischen Gruppen kann nicht nur zu Filterzwecken, sondern auch für andere Arbeiten wie z. B. das Erstellen von Berichten sehr hilfreich sein. Nähere Informationen zum Verwalten von Clients und Gruppen finden Sie im Kapitel Gruppen-Manager 53. Auch die Organisation von Clients mithilfe von Policies eignet sich für eine ganze Reihe von Einsatzzwecken. Nähere Informationen zum Erstellen und Verwalten von Policies finden Sie im Kapitel Policies 55.

Das erste Filterwerkzeug ist der Bereich zur Auswahl von Gruppen und Policies. Hier stehen drei Optionen zur Verfügung:

- **Clients in ausgewählten Objekten**
  Bewirkt, dass im Clientbereich nur die Clients in den ausgewählten Gruppen/Policies angezeigt werden.
- **Clients in nicht ausgewählten Objekten**
  Bewirkt, dass im Clientbereich nur die Clients in den nicht ausgewählten Gruppen/Policies sowie die Clients ohne Gruppen angezeigt werden.
- **Clients ohne Gruppen**
  Bewirkt, dass nur die Clients angezeigt werden, die keiner Gruppe/Policy angehören.

HINWEIS: Bei der Auswahl einer Gruppe aus der Liste werden auch alle dazugehörigen Untergruppen angezeigt.

Im unteren Teil des Filterbereichs können Sie weitere Kriterien definieren:
- **Filter - exakte Übereinstimmung**
  Es werden nur die Clients angezeigt, deren Name mit der angegebenen Zeichenfolge übereinstimmt.
- **Filter - Namensanfang (?,*)**
  Es werden nur die Clients angezeigt, deren Name mit der angegebenen Zeichenfolge anfängt.
- **Filter - Namensmuster (?,*)**
  Es werden nur die Clients angezeigt, deren Name die angegebene Zeichenfolge enthält.
- **Ausschlussfilter - exakte Übereinstimmung, Ausschlussfilter - Namensanfang (?,*), Ausschlussfilter - Namensmuster (?,*)**
  Diese Optionen funktionieren ähnlich wie die oben genannten drei Optionen, liefern jedoch jeweils das umgekehrte Ergebnis.

In den Feldern „Primärer Server", „Clientname", „Computername" und „MAC-Adresse" können Sie jeweils eine Suchzeichenfolge eingeben. Wenn in einem dieser Felder ein Wert eingetragen ist, werden die Ergebnisse der folgenden Datenbankabfrage auf der Grundlage dieses Werts gefiltert. Wenn mehrere Felder ausgefüllt sind, werden die Kriterien mit einem logischen UND verknüpft.

Als letzte Option können Sie einen Filter für Clients mit Problemen einrichten. Es werden dann nur Clients angezeigt, bei denen die angegebene Problemsituation vorliegt. Um die Liste der Problemsituationen anzuzeigen, aktivieren Sie die Option **Nur Probleme anzeigen** und klicken dann auf **Bearbeiten**. Wählen Sie die gewünschten Probleme aus und klicken Sie auf **OK**, um nur die Clients anzuzeigen, bei denen eine dieser Problemsituationen vorliegt.

Änderungen an den Filterkriterien werden übernommen, sobald Sie auf **Übernehmen** klicken. Um die Standardeinstellungen wiederherzustellen, klicken Sie auf **Zurücksetzen**. Wenn die Anzeige nach jeder Änderung an einem Filterkriterium automatisch aktualisiert werden soll, aktivieren Sie die Option **Extras** > **Konsolenoptionen** > **Sonstige Einstellungen** > **Änderungen automatisch übernehmen**.

3.3.2 Kontextmenü

Mit der rechten Maustaste können Sie das Kontextmenü aufrufen und die Ausgabe in den Anzeigespalten anpassen. Im Kontextmenü stehen die folgenden Optionen zur Verfügung:

- **Alle auswählen**
  Wählt alle Einträge aus.
- **Auswahl nach '...'**
  Wenn Sie mit der rechten Maustaste auf ein bestimmtes Attribut eines Eintrags klicken und dann diese Option wählen, werden alle Arbeitsplatzrechner bzw. Server ausgewählt, die ebenfalls dieses Attribut haben. Die Zeichenfolge „..." wird automatisch durch den Inhalt des betreffenden Attributs ersetzt.
- **Auswahl umkehren**
  Kehrt die aktuelle Auswahl der Einträge um.
- **Auswahl ausblenden**
  Blendet die ausgewählten Einträge aus.
- **Nur Auswahl anzeigen**
  Blendet alle nicht ausgewählten Einträge aus der Liste aus.

- **Spalten ein-/ausblenden**
  Öffnet das Fenster **Konsolenoptionen** > **Spalten - Anzeigen/Ausblenden**. Hier können Sie festlegen, welche Spalten im ausgewählten Fensterbereich angezeigt werden.

Die beiden Optionen **Auswahl ausblenden** und **Nur Auswahl anzeigen** sind besonders praktisch, wenn Sie die Anzeige

nach dem Anwenden von Filtern weiter einschränken möchten. Um alle über das Kontextmenü aktivierten Filter wieder zu deaktivieren, klicken Sie auf **Datei** > **Eingeschränkte Ansicht** oder auf das entsprechende Symbol in der ERAC-Symbolleiste. Sie können auch auf **F5** drücken, um die Anzeige zu aktualisieren und alle Filter zu deaktivieren.

Beispiel:

- So zeigen Sie nur Clients mit Bedrohungswarnungen an:
  Klicken Sie auf der Registerkarte **Clients** mit der rechten Maustaste auf einen beliebigen Eintrag, bei dem die Info „Letzte Bedrohungswarnung" leer ist. Klicken Sie dann im Kontextmenü auf **Auswahl nach '...'**. Öffnen Sie nun erneut das Kontextmenü und wählen Sie **Auswahl ausblenden**.

- So zeigen Sie ausschließlich Bedrohungswarnungen für die Clients „Josef" und „Karl" an:
  Klicken Sie auf die Registerkarte **Bedrohungen**. Klicken Sie dann mit der rechten Maustaste auf eine Zelle in der Spalte „Clientname", die den Wert „Josef" enthält. Öffnen Sie das Kontextmenü und wählen Sie **Auswahl nach 'Josef'**. Halten Sie die Strg-Taste gedrückt, wiederholen Sie den obigen Schritt für eine Zelle mit dem Inhalt „Karl" und wählen Sie dementsprechend **Auswahl nach 'Karl'**. Drücken Sie nun ein letztes Mal die rechte Maustaste, wählen Sie im Kontextmenü den Punkt **Nur Auswahl anzeigen** und lassen Sie die Strg-Taste los.

Mit der Strg-Taste können Sie gezielt mehrere Einzeleinträge nacheinander auswählen/abwählen, mit der Umschalttaste zusammenhängende Blöcke von Einträgen.

HINWEIS: Filter können Sie auch verwenden, um ohne großen Aufwand neue Tasks für eine ganz bestimmte Auswahl von Clients zu erstellen. Darüber hinaus gibt es noch viele weitere Möglichkeiten, um Filter effektiv bei Ihrer Arbeit einzusetzen. Probieren Sie die unterschiedlichen Möglichkeiten einfach einmal aus!

3.3.3 Anzeigemodus

Sie können einstellen, wie viele Spalten auf der Registerkarte **Clients** angezeigt werden. Verwenden Sie hierzu die Liste **Anzeigemodus** rechts in der Konsole. In der **Komplettansicht** werden alle Spalten angezeigt, in der **Minimalansicht** nur die wichtigsten. Diese vordefinierten Modi können nicht weiter bearbeitet werden. Zum Aktivieren der benutzerdefinierten Ansicht wählen Sie **Benutzerdefinierte Ansicht**. Diese Ansicht können Sie auf der Registerkarte **Extras** > **Konsolenoptionen** > **Spalten - Anzeigen/Ausblenden** weiter konfigurieren.

3.4 Registerkarten in ERAC

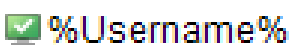
3.4.1 Allgemeiner Überblick zu Registerkarten und Clients

Die meisten Angaben auf den Registerkarten beziehen sich auf die Clients, die eine Verbindung zum Server aufgebaut haben. Jeder mit ERAS verbundene Client wird über die folgenden Attribute eindeutig identifiziert:
Computername (Clientname) + MAC-Adresse + Primärer Server

Wie sich ERAS bei bestimmten Verwaltungsaktionen im Netzwerk (z. B. Umbenennen eines PCs) verhält, können Sie in den erweiterten ERAS-Einstellungen festlegen. Auf diese Weise können Sie Dubletten auf der Registerkarte **Clients** vermeiden. Wenn beispielsweise einer der Computer im Netzwerk umbenannt wurde, die MAC-Adresse sich jedoch nicht geändert hat, können Sie dadurch verhindern, dass ein neuer Eintrag auf der Registerkarte **Clients** erstellt wird.

Clients, die erstmals eine Verbindung zu ERAS aufgebaut haben, sind durch den Wert **Ja** in der Spalte **Neuer Client** gekennzeichnet. Außerdem erscheint oben rechts am Clientsymbol ein kleines Sternchen (siehe die folgende Abbildung). Dadurch können Sie als Administrator neue Clients, die erstmals eine Verbindung aufgebaut haben, schnell erkennen. Je nach Ihren Vorgehensweisen bei der Administration kann dieses Attribut unterschiedliche Bedeutungen haben.

Nachdem Sie einen neuen Client konfiguriert und in eine bestimmte Gruppe verschoben haben, können Sie seine Kennzeichnung als neu löschen. Hierzu klicken Sie mit der rechten Maustaste auf den Client und wählen **Markierungen setzen/entfernen** > **Markierung „Neu" entfernen**. Das Clientsymbol erscheint dann wie in der folgenden Abbildung, und der Wert in der Spalte **Neuer Client** wechselt auf **Nein**.



HINWEIS: Das Attribut „Kommentar" ist auf allen drei Registerkarten optional. Hier können Sie eine beliebige

Beschreibung eintragen (z. B. „*Büro 129*“).

Zeitangaben in ERAS können entweder relativ („*Vor 2 Tagen*“), absolut („20.5.2009“) oder gemäß der Gebietseinstellungen des Systems angezeigt werden.

In den meisten Fällen können Sie die Daten durch Klicken auf einen Spaltenkopf auf- oder absteigend sortieren. Per Drag&Drop können Sie die Reihenfolge der Anzeigespalten verändern.

Durch Klicken auf bestimmte Werte können Sie zu anderen Registerkarten springen, um dort ausführlichere Informationen einzusehen. Wenn Sie beispielsweise auf einen Wert in der Spalte **Letzte Bedrohungswarnung** klicken, wird die Registerkarte **Bedrohungen** mit den Bedrohungs-Logeinträgen für den betreffenden Client angezeigt. Wenn Sie auf einen Wert klicken, dessen Detailinformationen aufgrund ihrer Menge nicht mehr in der Registerkartenansicht angezeigt werden können, erscheint ein Dialogfenster mit den Detailinformationen zum betreffenden Client.

3.4.2 Inhalt der Registerkarten bei Replikation

Wenn ERAC mit einem ERAS verbunden ist, dem weitere Server in einer Replikationsbeziehung untergeordnet sind, werden die Clients dieser untergeordneten Server automatisch angezeigt. Welche Daten repliziert werden, kann auf dem untergeordneten Server unter **Extras** > **Serveroptionen** > **Replikation** > **Einstellungen für ausgehende Replikation** konfiguriert werden.

In einem solchen Szenario fehlen zunächst eventuell die folgenden Daten:

- Ausführliche Log-Daten zu Bedrohungswarnungen (Registerkarte **Bedrohungen**)
- Ausführliche Log-Daten zu On-Demand-Scans (Registerkarte **Scans**)
- Ausführliche Client-Konfigurationsangaben im XML-Format (Spalten **Konfiguration**, **Schutzstatus**, **Schutzkomponenten** und **Systemeinformationen** auf der Registerkarte **Clients**)

Eventuell fehlen auch Daten aus ESET SysInspector. ESET SysInspector ist in ESET Produkten ab der Version 4.x enthalten.

Wenn die genannten Daten in den einzelnen Dialogfenstern nicht zur Verfügung stehen, klicken Sie auf die Schaltfläche **Anfordern** (unter **Aktionen** > **Eigenschaften** > **Konfiguration**). Hierdurch werden die fehlenden Daten vom untergeordneten ERAS angefordert. Da die Replikation immer vom untergeordneten ERAS eingeleitet wird, werden die fehlenden Daten innerhalb des eingestellten Replikationsintervalls übermittelt.

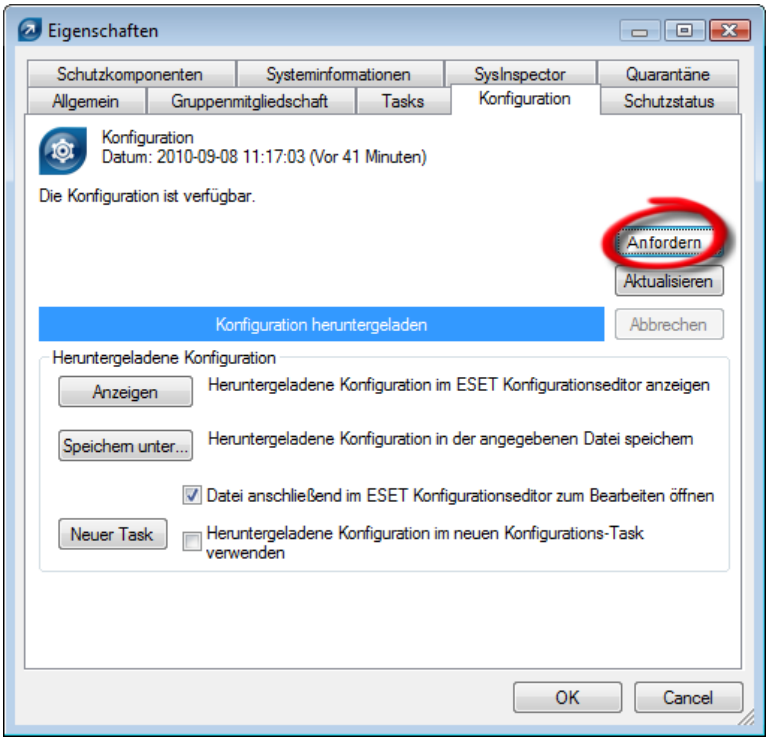


Abb.: Klicken Sie auf „Anfordern“, um fehlende Daten von untergeordneten ERA Servern abzurufen.

Auf dem übergeordneten Server können Sie festlegen, in welchem Umfang Logs entgegengenommen werden (**Extras** > **Serveroptionen** > **Erweitert** > **Erweiterte Einstellungen bearbeiten** > **ESET Remote Administrator** > **ERA Server** > **Einstellungen** > **Serverwartung** > **Umfang der entgegenzunehmenden ...-Logs**).

HINWEIS: Diese Option wirkt sich nicht nur auf die replizierten Clients aus, sondern auf alle Clients, die mit dem Server verbunden sind.

3.4.3 Clients (Registerkarte)

Diese Registerkarte zeigt allgemeine Informationen zu den einzelnen Clients.

Attribut	Beschreibung
Clientname	Name des Clients (kann im Eigenschaften-Dialogfenster des Clients auf der Registerkarte „Allgemein“ geändert werden)
Computername	Name des Arbeitsplatzrechners/Servers (Hostname)
MAC-Adresse	MAC-Adresse (Netzwerkadapter)
Primärer Server	Name des ERAS, zu dem der Client eine Verbindung aufgebaut hat
Domäne	Name der Domäne/Arbeitsgruppe, der der Client angehört (nicht identisch mit den in ERAS erstellten Gruppen)
IP	IP-Adresse
Produktname	Name des ESET Security-Produkts
Produktversion	Version des ESET Security-Produkts
Name der Policy	Name der Policy, die dem Client zugewiesen ist
Letzte Verbindung	Zeitpunkt, zu dem der Client zuletzt eine Verbindung mit ERAS aufgebaut hat (mit Ausnahme einiger Angaben, die per Replikation eingehen, tragen alle Daten, die vom jeweiligen Client erfasst werden, diesen Zeitstempel)
Schutzstatus-Text	Aktueller Status des auf dem Client installierten ESET Security-Produkts
Signaturdatenbank	Version der Signaturdatenbank
Letzte Bedrohungswarnung	Letzter Virenfund
Letzte Firewall-Warnung	Letztes Ereignis, das von der Personal Firewall aus ESET Smart Security erkannt wurde (es werden alle Ereignisse ab dem Schweregrad „Warnung“ angezeigt)
Letzte Ereigniswarnung	Letzte Fehlermeldung
Zuletzt geprüfte Dateien	Anzahl der Dateien, die beim letzten On-Demand-Scan geprüft wurden
Zuletzt infizierte Dateien	Anzahl der Dateien, die beim letzten On-Demand-Scan als infiziert erkannt wurden
Zuletzt gesäuberte Dateien	Anzahl der Dateien, die beim letzten On-Demand-Scan gesäubert (oder gelöscht) wurden
Letzter Scan	Zeitpunkt des letzten On-Demand-Scans
Neustart-Anforderung	Gibt an, ob ein Neustart erforderlich ist (z. B. nach einem Programmupgrade).
Zeitpunkt Neustart-Anforderung	Zeitpunkt der ersten Neustart-Anforderung
Letzter Produktstart	Zeitpunkt des letzten Starts des Clientprogramms
Produkt installiert (Zeitpunkt)	Zeitpunkt, zu dem das ESET Security-Produkt auf dem Client installiert wurde
Mobiler Benutzer	Wenn diese Einstellung bei einem Client aktiviert ist, wird bei jeder Verbindung des Clients zum ERAS ein Update-Task gestartet (empfohlen für Notebooks). Das Update findet nur statt, wenn die Signaturdatenbank des Clients nicht aktuell ist.
Neuer Client	Neu verbundener Computer (siehe hierzu das Kapitel Allgemeiner Überblick zu Registerkarten und Clients 23)
Betriebssystem	Name des Betriebssystems auf dem Client
Betriebssystem-Plattform	Plattform des Betriebssystems (Windows, Linux usw.)
Hardware-Plattform	32 oder 64 Bit
Konfiguration	Aktuelle XML-Konfiguration des Clients (mit Zeitpunkt ihrer Erstellung)
Schutzstatus	Allgemeine Angabe zum Status (ähnlich dem Attribut „Konfiguration“)
Schutzkomponenten	Allgemeine Angabe zum Status der Programmkomponenten (ähnlich dem Attribut „Konfiguration“)
Systeminformationen	Vom Client an ERAS übertragene Systeminformationen (mit Zeitpunkt der Übertragung)
SysInspector	Clients, auf denen eine Softwareversion installiert ist, die ESET SysInspector umfasst, können Logs aus dieser Zusatzanwendung an den Server übertragen.
Benutzerdefinierte Infos	Zusätzliche Infos, die vom Administrator für die Anzeige ausgewählt wurden (Einrichtung in ERAC über **Extras > Serveroptionen >** Registerkarte **Erweitert > Erweiterte Einstellungen bearbeiten > ESET Remote Administrator > ERA Server > Einstellungen > Sonstige Einstellungen > Benutzerdefinierte Clientinfos**).

Attribut	Beschreibung
Kommentar	Kurzer Kommentar zur Beschreibung des Clients (vom Administrator eingegeben)

HINWEIS: Einige Werte dienen nur zu Informationszwecken und spiegeln bei der Anzeige in der Konsole eventuell nicht den aktuellen Zustand des Clients wider. So könnte es zum Beispiel sein, dass eine Fehlermeldung zu einem Update vorliegt, das um 7:00 Uhr zwar fehlgeschlagen war, um 8:00 Uhr dann jedoch erfolgreich abgeschlossen wurde. Dies betrifft insbesondere die Infos **Letzte Bedrohungswarnung** und **Letzte Ereigniswarnung**. Wenn diese Infos bekanntermaßen nicht mehr aktuell sind, können Sie sie löschen. Klicken Sie hierzu mit der rechten Maustaste darauf und wählen Sie **Infos löschen** > **Info „Letzte Bedrohungswarnung" löschen** bzw. **Info „Letzte Ereigniswarnung" löschen**. Die Infos zum letzten Virenfund bzw. Systemereignis werden dann gelöscht.

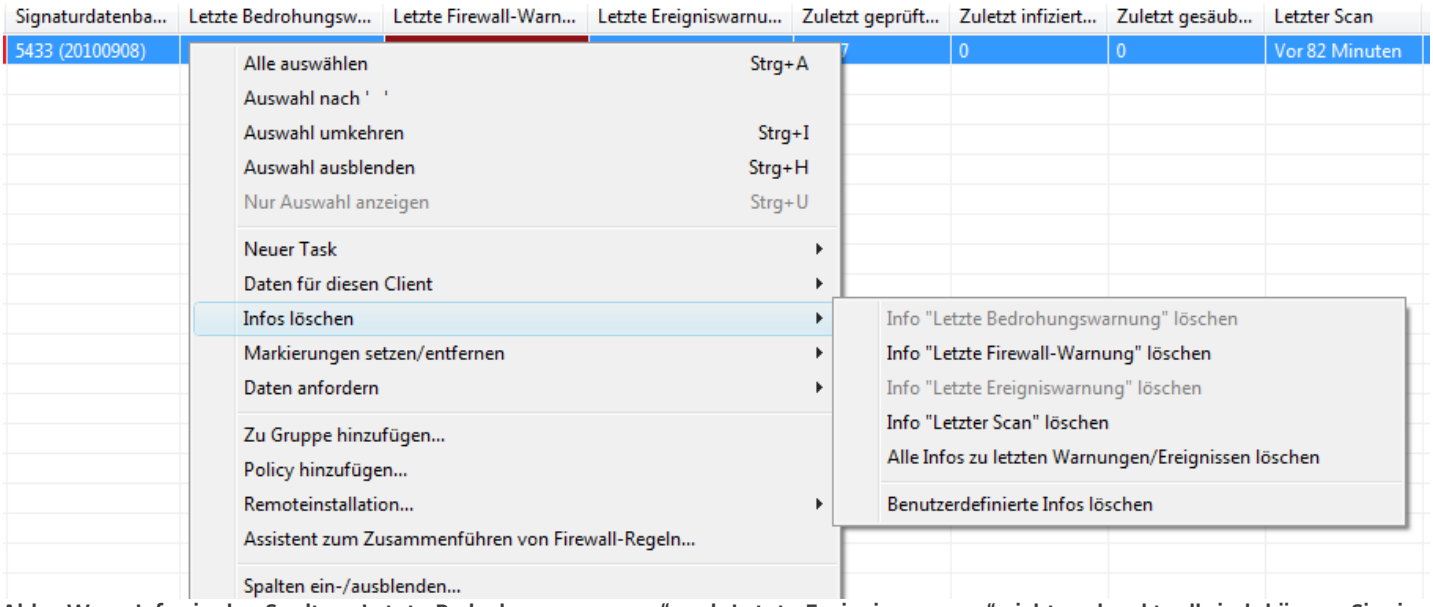


Abb.: Wenn Infos in den Spalten „Letzte Bedrohungswarnung" und „Letzte Ereigniswarnung" nicht mehr aktuell sind, können Sie sie leicht löschen.

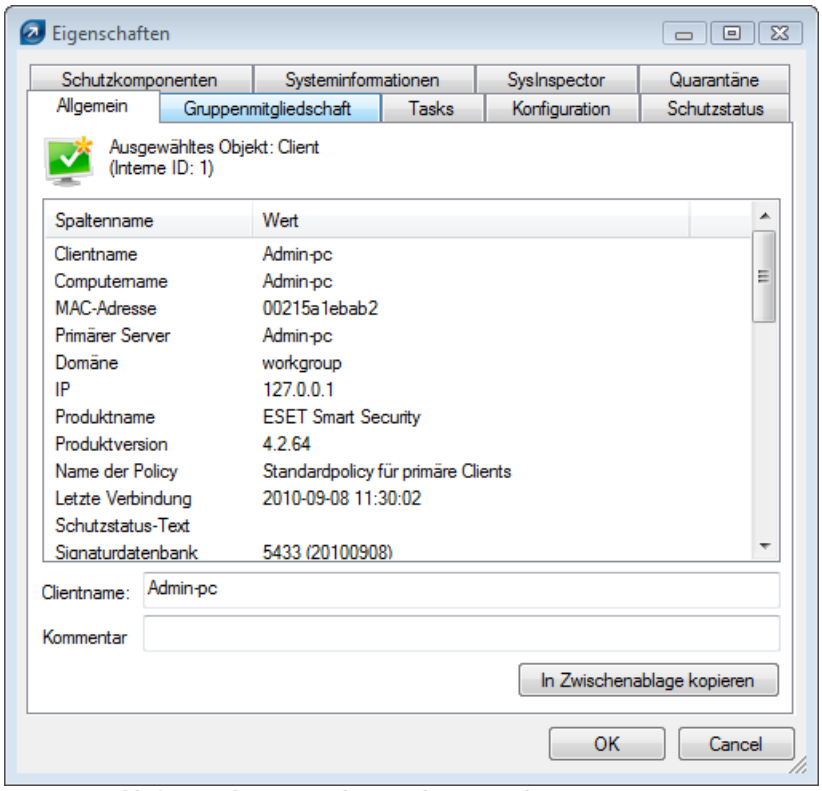


Abb.: Detailinformationen zu einem Client-Arbeitsplatzrechner.

Wenn Sie auf der Registerkarte **Clients** auf einen Client doppelklicken, erscheint ein Eigenschaften-Dialogfenster mit verschiedenen Optionen:

- **Allgemein**

Hier sehen Sie allgemeine Informationen zum Client (ähnlich wie auf der Registerkarte „Clients"). Außerdem können Sie

hier den Clientnamen festlegen, unter dem der Client in ERA angezeigt wird, sowie optional einen Kommentar eingeben.

- **Gruppenmitgliedschaft**
Diese Registerkarte zeigt alle Gruppen, denen der Client angehört. Nähere Informationen finden Sie im Kapitel Filtern von Informationen 21.

- **Tasks**
Tasks für den betreffenden Client. Nähere Informationen finden Sie im Kapitel Tasks 48.

- **Konfiguration**
Über diese Registerkarte können Sie sich die aktuelle Konfiguration des Clients anzeigen lassen oder in eine XML-Datei exportieren. In einem späteren Abschnitt dieses Handbuchs ist beschrieben, wie Sie mithilfe von XML-Dateien eine Konfigurationsvorlage zum Anlegen bzw. Ändern von XML-Konfigurationsdateien erstellen können. Nähere Informationen finden Sie im Kapitel Tasks 48.

- **Schutzstatus**
Hier finden Sie allgemeine Angaben zum Status aller installierten ESET Produkte. Teilweise sind diese Angaben interaktiv, sodass Sie direkt darauf reagieren können. Auf diese Weise müssen Sie nicht extra von Hand einen neuen Task definieren, um Probleme mit dem Schutzstatus zu beheben.

- **Schutzkomponenten**
Status der einzelnen ESET Security-Komponenten (Spamschutz, Personal Firewall usw.)

- **Systeminformationen**
Ausführliche Informationen zum installierten Programm, den Versionen der Programmkomponenten usw.

- **SysInspector**
Ausführliche Informationen zu Systemstart- und Hintergrundprozessen

- **Quarantäne**
Liste der Dateien in der Quarantäne. Sie können Dateien gezielt aus der Client-Quarantäne anfordern und auf einem lokalen Datenträger speichern.

3.4.4 Bedrohungen (Registerkarte)

Diese Registerkarte enthält ausführliche Informationen zu den einzelnen Virenfunden bzw. erkannten Bedrohungen.

Attribut	Beschreibung
Clientname	Name des Clients, der die Bedrohungswarnung gemeldet hat
Computername	Name des Arbeitsplatzrechners/Servers (Hostname)
MAC-Adresse	MAC-Adresse (Netzwerkadapter)
Primärer Server	Name des ERAS, zu dem der Client eine Verbindung aufgebaut hat
Empfangen	Zeitpunkt, zu dem das Ereignis von ERAS protokolliert wurde
Aufgetreten	Zeitpunkt, zu dem das Ereignis aufgetreten ist
Stufe	Schweregrad der Meldung
Scanner	Name der Schutzkomponente, die die Bedrohung erkannt hat
Objekt	Objekttyp
Name	In der Regel ein Ordner, in dem das infizierte Objekt abgelegt ist
Bedrohung	Name des erkannten Schadprogramms
Aktion	Aktion, die von der betreffenden Schutzkomponente ausgeführt wurde
Benutzer	Name des Benutzers, der zum Zeitpunkt des Ereignisses ermittelt wurde
Informationen	Informationen zur erkannten Bedrohung
Details	Übertragungsstatus des Client-Logs

3.4.5 Firewall (Registerkarte)

Diese Registerkarte zeigt Informationen zu den Firewall-Aktivitäten auf den Clients.

Attribut	Beschreibung
Clientname	Name des Clients, der das Ereignis gemeldet hat
Computername	Name des Arbeitsplatzrechners/Servers (Hostname)
MAC-Adresse	MAC-Adresse (Netzwerkadapter)
Primärer Server	Name des ERAS, zu dem der Client eine Verbindung aufgebaut hat
Empfangen	Zeitpunkt, zu dem das Ereignis von ERAS protokolliert wurde
Aufgetreten	Zeitpunkt, zu dem das Ereignis aufgetreten ist
Stufe	Schweregrad der Meldung
Ereignis	Beschreibung des Ereignisses
Quelle	IP-Quelladresse
Ziel	IP-Zieladresse
Protokoll	Protokoll der Verbindung
Regel	Verwendete Firewall-Regel
Anwendung	Betroffene Anwendung
Benutzer	Name des Benutzers, der zum Zeitpunkt des Ereignisses ermittelt wurde

3.4.6 Ereignisse (Registerkarte)

Diese Registerkarte zeigt eine Liste aller auf das System bezogenen Ereignisse.

Attribut	Beschreibung
Clientname	Name des Clients, der das Ereignis gemeldet hat
Computername	Name des Arbeitsplatzrechners/Servers (Hostname)
MAC-Adresse	MAC-Adresse (Netzwerkadapter)
Primärer Server	Name des ERAS, zu dem der Client eine Verbindung aufgebaut hat
Empfangen	Zeitpunkt, zu dem das Ereignis von ERAS protokolliert wurde
Aufgetreten	Zeitpunkt, zu dem das Ereignis aufgetreten ist
Stufe	Schweregrad der Meldung
Plugin	Name der Programmkomponente, die das Ereignis gemeldet hat
Ereignis	Beschreibung des Ereignisses
Benutzer	Name des Benutzers, der mit dem Ereignis verknüpft ist

3.4.7 Scans (Registerkarte)

Diese Registerkarte zeigt die Ergebnisse von On-Demand-Scans, die remote, lokal auf den Clientcomputern oder als geplante Tasks gestartet wurden.

Attribut	Beschreibung
Scan-ID	ID des entsprechenden Datenbankeintrags (im Format: *Scannummer*)
Clientname	Name des Clients, auf dem der Scan stattgefunden hat
Computername	Name des Arbeitsplatzrechners/Servers (Hostname)
MAC-Adresse	MAC-Adresse (Netzwerkadapter)
Primärer Server	Name des ERA Servers, zu dem der Client eine Verbindung aufgebaut hat
Empfangen	Zeitpunkt, zu dem das Scanereignis von ERAS protokolliert wurde
Aufgetreten	Zeitpunkt, zu dem der Scan auf dem Client stattgefunden hat
Geprüfte Objekte	Geprüfte Dateien, Ordner und Geräte
Geprüft	Anzahl der geprüften Dateien
Infiziert	Anzahl der infizierten Dateien
Gesäubert	Anzahl der gesäuberten (oder gelöschten) Objekte
Status	Status des Scans
Benutzer	Name des Benutzers, der zum Zeitpunkt des Ereignisses ermittelt wurde
Typ	Benutzertyp
Scanner	Scannertyp
Details	Übertragungsstatus des Client-Logs

3.4.8 Mobilgeräte (Registerkarte)

Diese Registerkarte zeigt ausführliche Log-Informationen von den Mobiltelefonen, die mit dem ERA Server verbunden sind.

Attribut	Beschreibung
Mobilgeräte-ID	Netzwerkkennung des Mobilgeräts
Clientname	Name des Clients, auf dem die Aktion stattgefunden hat
Computername	Name des Arbeitsplatzrechners/Servers (Hostname)
MAC-Adresse	MAC-Adresse (Netzwerkadapter)
Primärer Server	Name des ERA Servers, zu dem der Client eine Verbindung aufgebaut hat
Empfangen	Zeitpunkt, zu dem das Ereignis von ERAS protokolliert wurde
Aufgetreten	Zeitpunkt, zu dem das Ereignis auf dem Client stattgefunden hat
Stufe	Schweregrad der Meldung
Logtyp	Typ des Log-Eintrags (z. B. Sicherheits-Auditlog, SMS-Spamschutz-Log)
Ereignis	Beschreibung des Ereignisses
Objekttyp	Typ des Objekts, auf das sich das Ereignis bezieht (z. B. SMS, Datei ...)
Objektname	Objekt, auf das sich das Ereignis bezieht (z. B. Telefonnummer des SMS-Absenders, Dateipfad ...)
Aktion	Beim Ereignis ausgeführte Aktion (bzw. aufgetretener Fehler)

3.4.9 Quarantäne (Registerkarte)

Diese Registerkarte zeigt alle Quarantäneeinträge in Ihrem Netzwerk.

Attribut	Beschreibung
Quarantäne-ID	ID-Nummer des Quarantäneobjekts, vergeben in der Reihenfolge des Auftretens
Hash	Hashwert der Datei
Empfangen	Zeitpunkt, zu dem das Scanereignis von ERAS protokolliert wurde
Erstes Auftreten	Dauer seit dem ersten Auftreten des Quarantäneobjekts
Letztes Auftreten	Dauer seit dem letzten Auftreten des Quarantäneobjekts
Objektname	In der Regel ein Ordner, in dem das infizierte Objekt abgelegt ist
Dateiname	Name der Quarantänedatei
Erweiterung	Namenserweiterung der Quarantänedatei
Größe	Größe der Quarantänedatei
Grund	Grund für das Verschieben in die Quarantäne, in der Regel eine Beschreibung der Bedrohungsart
Clientanzahl	Anzahl der Clients, auf denen sich das Objekt in der Quarantäne befindet
Zugriffe	Gibt an, wie oft das Objekt in die Quarantäne verschoben wurde
Datei	Gibt an, ob ein Download des Objekts auf den Server angefordert wurde

3.4.10 Tasks (Registerkarte)

Ausführlichere Hintergrundinformationen zu dieser Registerkarte finden Sie im Kapitel „Tasks“. Sie umfasst die folgenden Attribute:

Attribut	Beschreibung
Status	Taskstatus („Aktiv“ = Task wird gerade übermittelt, „Abgeschlossen“ = Task wurde den Clients zugestellt)
Typ	Tasktyp
Name	Taskname
Beschreibung	Taskbeschreibung
Bereitstellungstermin	Zeitpunkt der Taskausführung
Empfangen	Zeitpunkt, zu dem das Ereignis von ERAS protokolliert wurde
Details	Übertragungsstatus des Task-Logs
Kommentar	Kurzer Kommentar zur Beschreibung des Clients (vom Administrator eingegeben)

3.4.11 Berichte (Registerkarte)

Mit den Funktionen auf dieser Registerkarte können Sie Angaben zu den Netzwerkaktivitäten in einem bestimmten Zeitraum archivieren. Die diesbezüglichen statistischen Daten können Sie als Grafiken und Diagramme aufbereiten. Nähere Informationen finden Sie im Kapitel Berichte 76.

3.4.12 Remoteinstallation (Registerkarte)

Über diese Registerkarte können Sie mit unterschiedlichen Methoden eine Remoteinstallation von ESET Smart Security oder ESET NOD32 Antivirus auf ausgewählten Clients durchführen. Ausführliche Informationen finden Sie im Kapitel Remoteinstallation 36.

3.5 Konfiguration von ERA Console

ERAC kann über den Menübefehl **Extras** > **Konsolenoptionen** konfiguriert werden.

3.5.1 Verbindung (Registerkarte)

Auf dieser Registerkarte wird die Verbindung von ERAC zu ERAS konfiguriert. Nähere Informationen finden Sie im Kapitel Verbindungsaufbau mit ERAS 19.

3.5.2 Spalten - Anzeigen/Ausblenden (Registerkarte)

Auf dieser Registerkarte können Sie festlegen, welche Attribute (Spalten) auf den einzelnen Registerkarten angezeigt werden. Die hier eingestellten Spalten beziehen sich auf die benutzerdefinierte Ansicht (Registerkarte **Clients**). Die Anzeige in den anderen Ansichtsmodi kann nicht geändert werden.

3.5.3 Farben (Registerkarte)

Auf dieser Registerkarte können Sie mit der so genannten „bedingten Hervorhebung“ einzelnen Systemereignissen unterschiedliche Farben zuordnen, um Clients, bei denen ein Problem vorliegt, deutlicher sichtbar zu machen. Auf diese Weise können Sie beispielsweise Clients, auf denen die Signaturdatenbank noch einigermaßen aktuell ist (**Clients: Vorgängerversion**) farblich von Clients mit einer veralteten Signaturdatenbank unterscheiden (**Clients: Ältere Version oder nicht verfügbar**).

3.5.4 Pfade (Registerkarte)

Auf diese Registerkarte können Sie festlegen, in welchem Verzeichnis ERAC die von ERAS heruntergeladenen Berichte speichert. Standardmäßig ist dies das folgende Verzeichnis:

%ALLUSERSPROFILE%\Anwendungsdaten\Eset\ESET Remote Administrator\Console\reports

3.5.5 Datum/Uhrzeit (Registerkarte)

Anzeigeformat von Spalten mit Datum/Uhrzeit:

- **Absolute Zeitangaben**
  Bewirkt, dass in der Konsole absolute Zeitangaben angezeigt werden (z. B. „*14:30:00*“).

- **Relative Zeitangaben**
  Bewirkt, dass in der Konsole relative Zeitangaben angezeigt werden (z. B. „*Vor zwei Wochen*“).

- **Format aus den Gebietseinstellungen verwenden**
  Bewirkt, dass Zeitangaben in der Konsole gemäß der Gebietseinstellungen aus der Windows-Systemsteuerung angezeigt werden.

- **UTC-Angaben in Ortszeit umrechnen**
  Aktivieren Sie dieses Kontrollkästchen, damit Zeitangaben in Ihre Ortszeit umgerechnet werden. Ansonsten werden Zeitangaben in GMT/UTC verwendet.

3.5.6 Sonstige Einstellungen (Registerkarte)

- **Filtereinstellungen** > **Änderungen automatisch übernehmen**
  Wenn diese Option aktiviert ist, wird bei jeder Änderung an den Filtereinstellungen für eine bestimmte Registerkarte die Anzeige sofort aktualisiert. Ansonsten wird der neue Filter erst übernommen, wenn Sie auf **Übernehmen** klicken.

- **Remote Administrator-Updates**
  In diesem Bereich können Sie die Suche nach neuen Versionen von ESET Remote Administrator aktivieren. Die Standardeinstellung **Monatlich** wird empfohlen. Wenn eine neue Version verfügbar ist, zeigt ERAC beim Programmstart eine entsprechende Meldung an.

- **Sonstige Einstellungen** > **Anzeige automatisch alle ... Min. aktualisieren**
  Wenn diese Option aktiviert ist, wird die Anzeige auf den einzelnen Registerkarten automatisch im festgelegten Zeitintervall aktualisiert.

- **Sonstige Einstellungen** > **Gitternetzlinien anzeigen**
  Wenn Sie diese Option aktivieren, werden die Zellen auf den einzelnen Registerkarten durch Gitternetzlinien voneinander getrennt.

- **Sonstige Einstellungen** > **Clients im Format „Server/Name" statt „Server/Computer/MAC" anzeigen**
  Legt das Anzeigeformat für Clienteinträge in bestimmten Dialogfenstern fest (z. B. „Neuer Task"). Diese Option wirkt sich ausschließlich auf die Anzeige aus.

- **Sonstige Einstellungen** > **Symbol im Infobereich der Taskleiste anzeigen**
  Wenn diese Option aktiviert ist, wird ein Symbol für ERA Console im Infobereich der Windows-Taskleiste angezeigt.

- **Sonstige Einstellungen** > **Im minimierten Zustand auf der Taskleiste anzeigen**
  Bewirkt, dass ERAC weiterhin in der Windows-Taskleiste erscheint, auch wenn das Programmfenster minimiert ist.

- **Sonstige Einstellungen** > **Taskleisten-Symbol hervorheben, wenn Clients mit Problemen gefunden werden**
  Diese Option bewirkt, dass das ERAC-Symbol im Infobereich der Taskleiste seine Farbe ändert, wenn bestimmte Problemsituationen vorliegen. Diese Situationen können Sie über die Schaltfläche „Bearbeiten" definieren.

Wenn ERAC vom Administrator-PC aus ständig mit einem ERAS verbunden bleiben soll, empfiehlt es sich, die Option **Im minimierten Zustand auf der Taskleiste anzeigen** zu aktivieren und die Konsole zu minimieren, wenn gerade nicht damit gearbeitet wird. Bei einem Problem erscheint das Programmsymbol im Infobereich der Taskleiste rot, um zu zeigen, dass Handlungsbedarf besteht. Bei welchen Problemsituationen dies geschieht, können Sie über die Einstellungen für die Option **Taskleisten-Symbol hervorheben, wenn Clients mit Problemen gefunden werden** einrichten. Beachten Sie allerdings, dass ERAC die Verbindung trennt, wenn die Datenbankkomprimierung auf dem Server aktiviert wird.

- **Sonstige Einstellungen** > **Optionale Informationsmeldungen**
  Hiermit können Sie alle Informationsmeldungen deaktivieren („Alle deaktivieren") oder aktivieren („Alle aktivieren").

3.6 Anzeigemodi

In ERAC haben Sie die Wahl zwischen zwei Anzeige- bzw. Zugriffsmodi:

- Administratormodus
- Read-Only-Modus (Lesemodus)

Im Administratormodus können Sie in ERAC uneingeschränkt auf alle Funktionen und Einstellungen zugreifen sowie alle verbundenen Clients verwalten.

Der Read-Only-Modus eignet sich, um den Status der ESET Clientsoftware auf den mit dem ERAS verbundenen Clients zu überwachen. Sie können in diesem Modus jedoch keine Tasks für die Client-Arbeitsplatzrechner anlegen, Installationspakete erstellen oder Remoteinstallationen durchführen. Auch der Zugriff auf den Lizenz-, Policy- und Notifikations-Manager ist gesperrt. Sie können im Read-Only-Modus allerdings weiterhin die ERAC-Einstellungen bearbeiten und Berichte erstellen.

Den Anzeigemodus für eine Sitzung wählen Sie beim Start der Konsole über die Liste **Zugriff** aus. Das Passwort für den Verbindungsaufbau zu ERAS kann für jeden der beiden Modi separat festgelegt werden. Diese Möglichkeit ist besonders praktisch, wenn bestimmte Benutzer Vollzugriff auf ERAS erhalten sollen, andere hingegen nur Read-Only-

Zugriff (Lesezugriff). Um die Passwörter einzurichten, klicken Sie auf **Extras** > **Serveroptionen** > **Sicherheit** und dann auf die Schaltfläche **Ändern** neben „Passwort für Konsole (Administratorzugriff)“ bzw. „... (Read-Only-Zugriff)“.

3.7 ESET Configuration Editor

Der ESET Configuration Editor ist eine wichtige Komponente von ERAC und wird für verschiedene Zwecke verwendet. Insbesondere dient er zum Erstellen von:

- Vordefinierten Konfigurationen für Installationspakete
- Konfigurationen, die über Tasks oder Policies an die Clients übermittelt werden
- Allgemeine Konfigurationsdateien im .xml-Format

Der Configuration Editor ist ein Teil von ERAC und besteht hauptsächlich aus den Dateien *cfgedit.**.

Über den Configuration Editor können Sie als Administrator viele Parameter der ESET Security-Produkte zentral aus der Ferne konfigurieren. Praktisch wird dies insbesondere für die Produkte relevant sein, die auf den Client-Arbeitsplatzrechnern installiert sind. Fertige Konfigurationen können Sie als .xml-Dateien exportieren, um sie später an unterschiedlicher Stelle zu verwenden, etwa zum Erstellen von Tasks in ERAC, zum lokalen Import einer Konfiguration in ESET Smart Security usw.

Als Struktur verwendet der Configuration Editor eine *.xml*-Vorlage, in der die Konfiguration als Baumstruktur gespeichert wird. Diese Vorlage ist in der Datei *cfgedit.exe* gespeichert. Daher empfiehlt es sich, regelmäßige Updates von ERAS und ERAC durchzuführen.

Warnung: Im Configuration Editor können Sie beliebige *.xml*-Dateien bearbeiten. Achten Sie darauf, nicht die Vorlage *cfgedit.xml* zu ändern oder zu überschreiben.

Zur ordnungsgemäßen Funktion des Configuration Editor müssen die folgenden Dateien vorhanden sein: *eguiEpfw.dll*, *cfgeditLang.dll*, *eguiEpfwLang.dll* sowie *eset.chm*.

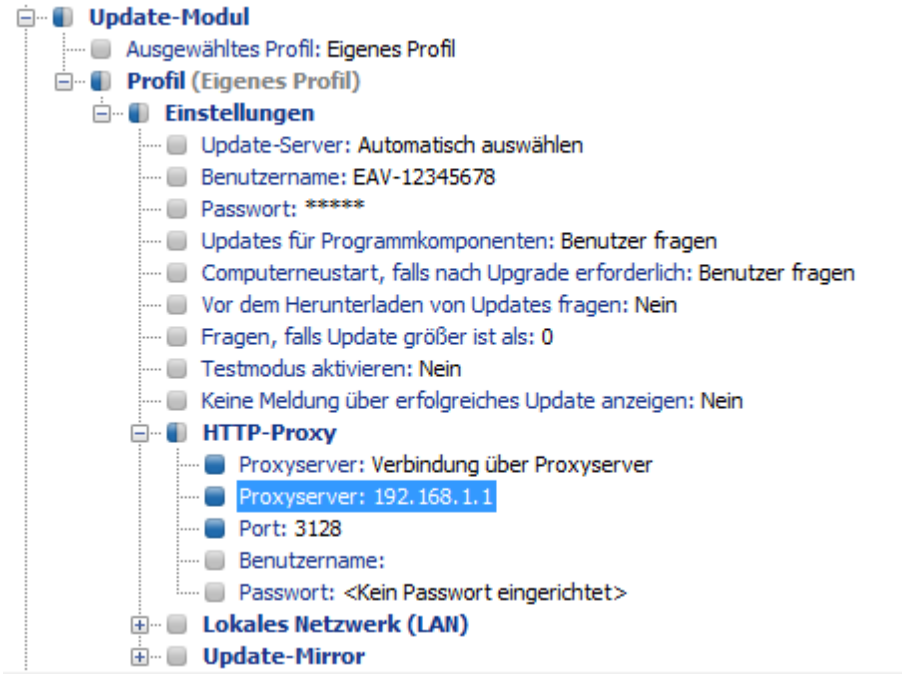
3.7.1 Arbeiten mit mehreren Konfigurationsebenen

Wenn Sie einen Wert im Configuration Editor ändern, wird die betreffende Einstellung mit einem blauen Symbol versehen. Einträge mit einem grauen Symbol wurden nicht verändert und werden daher auch nicht in die *.xml*-Ausgabekonfiguration geschrieben.

Bei der Übernahme einer Konfiguration auf einem Client werden nur diejenigen Änderungen übernommen, die in der *.xml*-Datei mit der Ausgabekonfiguration gespeichert wurden (). Alle anderen Einträge () bleiben unverändert. Auf diese Weise können Sie schrittweise mehrere Konfigurationsebenen nacheinander anwenden, ohne dass sich diese gegenseitig aufheben.

Ein Beispiel können Sie der nachstehenden Abbildung entnehmen. In dieser Konfiguration werden der Benutzername *EAV-12345678* und das Passwort festgelegt sowie die Nutzung eines Proxyservers unterbunden.

Wenn nun in einem zweiten Schritt zusätzlich die nachstehend abgebildete Konfiguration an die Clients übertragen wird, bleiben die bisherigen Änderungen mit dem Benutzernamen *EAV-12345678* und dem Passwort erhalten. Zusätzlich lässt die Konfiguration jedoch die Nutzung eines Proxyservers zu und definiert dessen Adresse und Port.



3.7.2 Wesentliche Konfigurationseinträge

Dieser Abschnitt erläutert einige der wesentlichen Konfigurationseinträge für ESET Smart Security und ESET NOD32 Antivirus, die über den ESET Configuration Editor zur Verfügung stehen:

- **ESET Smart Security**, **ESET NOD32 Antivirus** > **ESET-Kernel** > **Einstellungen** > **Remote Administration**
  Hier können Sie die Kommunikation zwischen den Clientcomputern und ERAS aktivieren (**Remote Administrator Server verwenden**). Geben Sie den Namen oder die IP-Adresse des ERAS-Rechners ein (**Adresse des primären Servers**). Die Einstellung **Intervall für Verbindungsaufnahme zum Server** sollte auf dem Standardwert 5 Minuten belassen werden. Zu Testzwecken können Sie diesen Wert auf 0 herabsetzen, was bewirkt, dass alle 10 Sekunden eine Verbindung aufgebaut wird. Falls in ERAS ein Passwort für die Verbindungsaufnahme eingerichtet ist, tragen Sie es ein. Nähere Informationen finden Sie in der Beschreibung der Option **Passwort für Clients** im Kapitel Sicherheit (Registerkarte) 79. Dieser Abschnitt enthält auch weitere Informationen zum Konfigurieren des Passworts.

- **ESET-Kernel** > **Einstellungen** > **Lizenzschlüssel**
  Auf Clientcomputern müssen keine Lizenzschlüssel hinzugefügt oder verwaltet werden. Lizenzschlüssel werden nur für Serverprodukte verwendet.

- **ESET-Kernel** > **Einstellungen** > **ThreatSense.Net**
  Dieser Zweig steuert das Verhalten des Frühwarnsystems ThreatSense.Net, über das Sie verdächtige Dateien zur Analyse an ESET weiterleiten können. Bei der Bereitstellung von ESET Lösungen in einem großen Netzwerk sind besonders die Optionen **Verdächtige Dateien einreichen** und **Anonyme statistische Informationen einreichen** wichtig. Wenn diese Einstellungen auf **Nicht zur Analyse einreichen** bzw. **Nein** gesetzt sind, wird ThreatSense.Net komplett deaktiviert. Um Dateien automatisch und ohne Benutzereingriff einzureichen, wählen Sie **Ohne Nachfrage automatisch einreichen** bzw. **Ja**. Wenn die Internetverbindung über einen Proxyserver läuft, legen Sie unter **ESET-Kernel > Einstellungen > Proxyserver** die entsprechenden Parameter fest.
  Standardmäßig übermitteln die Clientprodukte verdächtige Dateien zunächst an ERAS. Von dort werden sie dann an die ESET-Server weitergeleitet. Auch in ERAS muss daher ein eventuell vorhandener Proxyserver korrekt eingerichtet sein (**Extras > Serveroptionen > Erweitert > Erweiterte Einstellungen bearbeiten > ERA Server > Einstellungen > Proxyserver**).

- **ESET-Kernel** > **Einstellungen** > **Einstellungen mit Passwort schützen**
  Hiermit können Sie als Administrator die Konfigurationsparameter mit einem Passwort schützen. Wenn ein Passwort gesetzt ist, ist ein Zugriff auf die Konfiguration auf den Client-Arbeitsplatzrechnern nur noch mit diesem Passwort möglich. Auf Konfigurationsänderungen, die in ERAC vorgenommen werden, hat dieses Passwort jedoch keinen Einfluss.

- **ESET-Kernel** > **Einstellungen** > **Taskplaner**
  Dieser Zweig enthält die Taskplaner-Einstellungen, über die Sie beispielsweise eine regelmäßige Systemprüfung o. ä. einrichten können.

HINWEIS: Standardmäßig sind in allen ESET Security-Lösungen bereits einige Tasks vordefiniert (z. B. regelmäßige automatische Updates und die automatische Prüfung wichtiger Dateien beim Start). In den meisten Fällen sollte es nicht erforderlich sein, diese Tasks zu bearbeiten oder neue zu definieren.

- **ESET-Kernel** > **Einstellungen** > **Standardwerte für Benutzeroberfläche**
  Mit diesen Einstellungen (z. B. **Startbild anzeigen** ja/nein) werden lediglich die Standardeinstellungen der Clients angepasst. Benutzer auf den Clients können die Einstellungen anschließend individuell anpassen. Eine Änderung per Remoteverwaltung ist dann standardmäßig nicht mehr möglich. Um Remoteänderungen zu ermöglichen, müssen Sie die Option **Benutzereinstellungen überschreiben** auf **Ja** setzen. Die Option **Benutzereinstellungen überschreiben** ist nur für Clients mit ESET Security-Produkten ab der Version 4.0 verfügbar.

- **Update-Modul**
  Über diesen Zweig richten Sie die Update-Profile ein. In der Regel müssen Sie nur die Einstellungen **Update-Server**, **Benutzername** und **Passwort** im vordefinierten Profil **Eigenes Profil** anpassen. Wenn für die Update-Server-Einstellung die Option **Automatisch auswählen** aktiv ist, werden alle Updates von den ESET Update-Servern heruntergeladen. In diesem Fall tragen Sie bitte den **Benutzernamen** und das **Passwort** ein, die Sie beim Kauf erhalten haben. Sie können die Client-Arbeitsplatzrechner auch so einrichten, dass Updates von einem lokalen Server (Mirror) abgerufen werden. Nähere Informationen hierzu finden Sie im Kapitel Mirror-Server 80. Nähere Informationen zur Arbeit mit dem Taskplaner finden Sie im Kapitel Taskplaner 94.

HINWEIS: Auf tragbaren Geräten wie beispielsweise Notebooks können zwei Profile konfiguriert werden - eins zum Abruf von Updates über den Mirror-Server, eins zum direkten Download von den ESET-Servern. Nähere Informationen

finden Sie im Kapitel Kombinierter Update-Abruf für Notebooks 98 am Ende dieses Dokuments.

4. Installation von ESET Clientlösungen

Dieses Kapitel beschäftigt sich mit der Installation von ESET Clientlösungen unter Microsoft Windows. Eine solche Installation kann direkt vor Ort an den Arbeitsplatzrechnern oder remote über ERAS durchgeführt werden. Darüber hinaus beschreibt dieses Kapitel weitere Alternativen für die Remoteinstallation.

HINWEIS: Die Remoteinstallation von ESET Produkten auf Servern ist zwar technisch möglich, wird aber nicht empfohlen. Nutzen Sie diese Funktion nach Möglichkeit nur für Arbeitsplatzrechner.

4.1 Direkte Installation

Bei einer direkten Installation sitzt der Administrator vor Ort an dem Computer, auf dem das ESET Security-Produkt installiert werden soll. Für diese Methode ist keine weitere Vorbereitung erforderlich. Sie eignet sich für kleine Netze und für Szenarien, in denen ERA nicht verwendet wird.

Deutlich vereinfachen lässt sich eine solche Installation mithilfe einer vordefinierten .xml-Konfiguration. Während und nach der Installation sind dann keine weiteren Anpassungen an der Konfiguration erforderlich, etwa zum Einrichten eines Update-Servers (Benutzername/Passwort, Pfad zum Mirror-Server usw.), zum Aktivieren des „stillen Modus", für geplante Scans usw.

Je nach verwendeter Version der ESET Clientlösungen (4.x, 3.x oder 2.x) wird die .xml-Konfigurationsdatei auf unterschiedliche Weise übergeben:

- Version 4.x: Laden Sie die Installationsdatei (z. B. *ess_nt32_enu.msi*) von *eset.com* herunter und erstellen Sie im **Installationspaket-Editor** ein eigenes Installationspaket. Erstellen oder wählen Sie die Konfiguration, die Sie mit diesem Paket verknüpfen möchten. Klicken Sie neben dem Feld **Paket für Windows NT-Systeme (xx Bit)** auf **Kopieren** und speichern Sie das Paket im Format **ESET-MSI-Installationspaket mit Konfiguration (*.msi)**.

  HINWEIS: Durch das Hinzufügen einer Konfiguration zur *.msi*-Installationsdatei wird die digitale Signatur dieser Datei ungültig.

  Führen Sie außerdem auch unter der Version 4.x die für die Version 3.x genannten Schritte aus.

- Version 3.x: Laden Sie die Installationsdatei (z. B. *ess_nt32_enu.msi*) von *eset.com* herunter. Kopieren Sie die Konfigurationsdatei (*cfg.xml*) in das Verzeichnis, in dem die Installationsdatei gespeichert ist. Wenn Sie nun die Installationsdatei starten, wird automatisch die Konfiguration aus der *.xml*-Konfigurationsdatei übernommen. Wenn die *.xml*-Konfigurationsdatei einen anderen Namen hat oder an einem anderen Speicherort liegt, können Sie den Parameter *ADMINCFG ="Pfad_zur_XML-Datei"* verwenden (Beispiel: *ess_nt32_enu.msi ADMINCFG ="\\server\xml\settings.xml"* für eine Konfiguration auf einem Netzlaufwerk).

- Version 2.x: Laden Sie die Installationsdatei (z. B. *ndntenst.exe*) von *eset.com* herunter. Entpacken Sie die heruntergeladene Datei mit einem Packer wie WinRAR in einen Ordner. Dieser Ordner enthält dann die Installationsdateien, insbesondere die *setup.exe*. Kopieren Sie die Konfigurationsdatei *nod32.xml* in den Ordner. Starten Sie die Datei *setup.exe*. Die Konfiguration aus der Datei *nod32.xml* wird nun automatisch übernommen. Wenn die *.xml*-Konfigurationsdatei einen anderen Namen hat oder an einem anderen Speicherort liegt, können Sie den Parameter *ADMINCFG ="Pfad_zur_XML-Datei"* verwenden. (Beispiel: *setup.exe /cfg ="\\server\xml\settings.xml"* für eine Konfiguration auf einem Netzlaufwerk)

4.2 Remoteinstallation

ERA bietet verschiedene Methoden zum Durchführen einer Remoteinstallation. Für die Verteilung der Installationspakete auf die gewünschten Arbeitsplatzrechner gibt es die folgenden Möglichkeiten:

- Push-Remoteinstallation
- Remoteinstallation per Anmeldeskript
- Remoteinstallation per E-Mail
- Upgrade

Eine Remoteinstallation über ERA umfasst die folgenden Schritte:

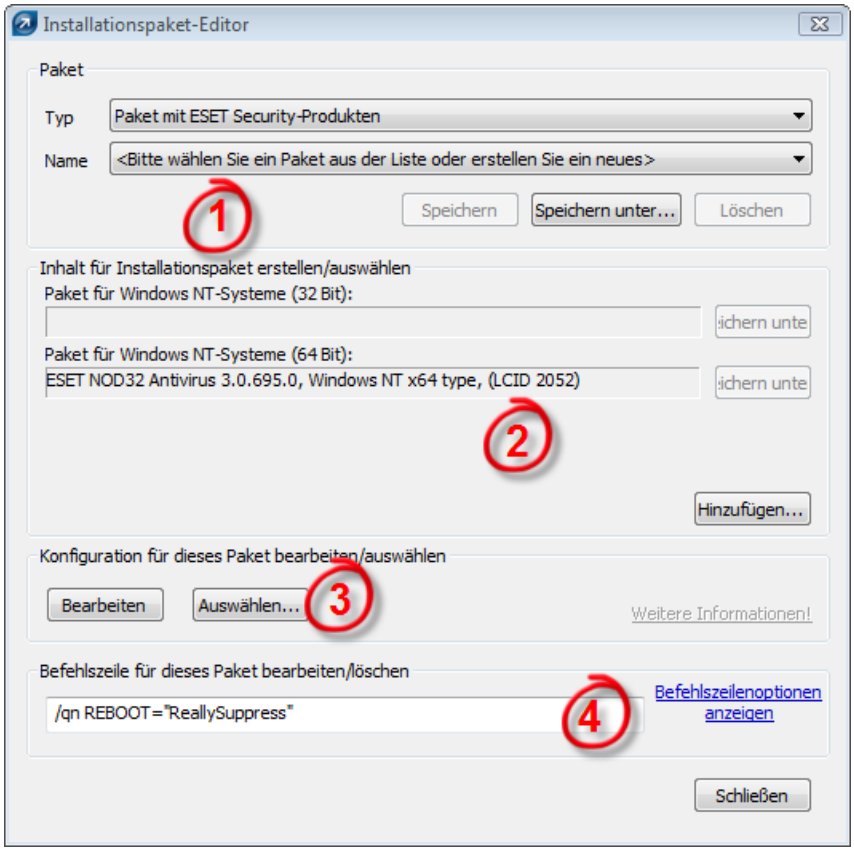
- Erstellen der Installationspakete
- Verteilen der Pakete auf die Client-Arbeitsplatzrechner (per Push-Installation, Anmeldeskript, E-Mail, Upgrade oder

über eine externe Lösung)

Der erste Schritt wird über ERAC ausgelöst. Das Installationspaket selbst liegt jedoch auf dem ERAS im folgenden Verzeichnis:

%ALLUSERSPROFILE%\Anwendungsdaten\Eset\ESET Remote Administrator\Server\packages

Zum Verwalten der Installationspakete in ERAC klicken Sie auf die Registerkarte **Remoteinstallation**, wählen die Registerkarte **Computer** und klicken dort mit der rechten Maustaste auf eine beliebige Stelle. Wählen Sie nun im Kontextmenü den Punkt **Pakete verwalten**.



Jedes Installationspaket wird durch einen Namen eindeutig gekennzeichnet (siehe Punkt 1 in der oben stehenden Abbildung). Die restlichen Bereiche des Dialogfensters beziehen sich auf den Inhalt des Pakets, der installiert wird, nachdem das Paket auf den gewünschten Arbeitsplatzrechner übertragen wurde. Jedes Paket enthält:

- Installationsdateien für die gewünschte ESET Clientsoftware (2)
- eine *.xml*-Konfigurationsdatei für die ESET Clientsoftware (3)
- Befehlszeilenparameter für das Paket (4)

Über die Liste **Typ** im Bereich 1 können Sie auf weitere ERA-Funktionen zugreifen. Neben der Möglichkeit zur Remoteinstallation können ESET Security-Produkte über die Option **ESET Security-Produkte und NOD32 Version 2 deinstallieren** auch remote deinstalliert werden. Über die Option **Benutzerdefiniertes Paket** können Sie außerdem eine Remoteinstallation einer externen Anwendung durchführen. Diese Möglichkeit ist sehr hilfreich, um beliebige Skripts und Programme auf dem Remoterechner auszuführen, zum Beispiel Deinstallationsroutinen für Security-Software anderer Hersteller oder Standalone-Tools zum Entfernen bestimmter Infektionen. Dabei können Sie eine bestimmte Datei als **Einstiegsdatei** definieren und dieser beliebige Befehlszeilenparameter übergeben. Nähere Informationen finden Sie im Kapitel Installation von Produkten anderer Hersteller über ERA 99.

In jedes Paket wird automatisch ein ESET Remote Installer-Agent integriert, der die Installation sowie die Kommunikation zwischen dem Zielrechner und ERAS abwickelt. Dieser Agent hat den Dateinamen *einstaller.exe* und enthält sowohl den ERAS-Namen als auch den Namen und Typ des dazugehörigen Pakets. Die folgenden Kapitel beschreiben den Agenten im Detail.

Sie können den Installationsvorgang mit einer Reihe von Parametern steuern. Diese können sowohl bei einer direkten Installation (Administrator sitzt vor dem Arbeitsplatzrechner) als auch bei einer Remoteinstallation verwendet werden. Bei einer Remoteinstallation werden die Parameter bei der Konfiguration des Installationspakets festgelegt und später automatisch der Installationsroutine auf dem Zielrechner übergeben. Um zusätzliche Parameter bei der Installation von ESET Smart Security oder ESET NOD32 Antivirus zu verwenden, geben Sie sie nach dem Namen des *.msi*-Installationspakets ein (Beispiel: *eav_nt64_ENU.msi /qn*). Die folgenden Parameter stehen zur Verfügung:

- **/qn**
  Unbeaufsichtigte Installation (es werden keine Dialogfenster angezeigt).
- **/qb!**
  Es sind keine Benutzereingriffe möglich, der Verlauf der Installation wird jedoch über eine Fortschrittsleiste (Prozentanzeige) angezeigt.
- **REBOOT ="ReallySuppress"**
  Bewirkt, dass nach der Installation des Programms kein Neustart stattfindet.
- **REBOOT ="Force"**
  Führt nach der Installation automatisch einen Neustart durch.
- **REBOOTPROMPT =""**
  Bewirkt, dass nach der Installation ein Dialogfenster angezeigt wird, in dem der Benutzer gebeten wird, den Neustart zu bestätigen (kann nicht mit dem Parameter */qn* kombiniert werden).
- **ADMINCFG ="(XML-Dateipfad)"**
  Übergibt der Installationsroutine des ESET Security-Produkts die Parameter aus der angegebenen XML-Datei. Bei einer Remoteinstallation ist dieser Parameter nicht erforderlich. Jedes Installationspaket enthält eine eigene *.xml*-Konfigurationsdatei, die automatisch verwendet wird.
- **PASSWORD="(Passwort)"**
  Diesen Parameter müssen Sie hinzufügen, wenn die ESS-/EAV-Einstellungen durch ein Passwort geschützt sind.

Bei ESET NOD32 Antivirus 2.x sind die Parameter der Datei *setup.exe* zu übergeben, die gemeinsam mit den anderen Dateien aus dem Installationspaket entpackt werden kann (Beispiel: *setup.exe /silentmode*). Die folgenden Parameter stehen zur Verfügung:

- **/SILENTMODE**
  Unbeaufsichtigte Installation (es werden keine Dialogfenster angezeigt).
- **/FORCEOLD**
  Erzwingt die Installation einer älteren Version über eine ggf. installierte neuere Version.
- **/CFG ="(XML-Dateipfad)"**
  Übergibt der Installationsroutine des ESET Security-Produkts die Parameter aus der angegebenen *.xml*-Datei. Bei einer Remoteinstallation ist dieser Parameter nicht erforderlich. Jedes Installationspaket enthält eine eigene *.xml*-Konfigurationsdatei, die automatisch verwendet wird.
- **/REBOOT**
  Führt nach der Installation automatisch einen Neustart durch.
- **/SHOWRESTART**
  Bewirkt, dass nach der Installation ein Dialogfenster angezeigt wird, in dem der Benutzer gebeten wird, den Neustart zu bestätigen. Dieser Parameter kann nur gemeinsam mit dem Parameter *SILENTMODE* verwendet werden.
- **/INSTMFC**
  Installiert die MFC-Bibliotheken für Microsoft Windows 9x, die für eine korrekte Funktion von ERA erforderlich sind. Dieser Parameter kann auch dann verwendet werden, wenn die MFC-Bibliotheken bereits installiert sind.

Über den Bereich **Inhalt für Installationspaket erstellen/auswählen** können Sie ein Standalone-Installationspaket mit einer vordefinierten Konfiguration aus einem bereits vorhandenen, gespeicherten Installationspaket (Schaltfläche **Speichern unter**) erstellen. Dieses Installationspaket kann dann auf dem Client-Arbeitsplatzrechner ausgeführt werden, auf dem das Programm installiert werden soll. Der Anwender auf dem Clientrechner muss zur Installation lediglich das Paket ausführen. Eine Verbindung zu ERAS ist hierfür nicht erforderlich.

HINWEIS: Durch das Hinzufügen einer Konfiguration zur *.msi*-Installationsdatei wird die digitale Signatur dieser Datei ungültig.

Wichtig: Unter Microsoft Windows Vista und neueren Versionen wird für die Remoteinstallation dringend der unbeaufsichtigte Installationsmodus empfohlen (Parameter */qn*, */qb*). Ansonsten kann die Interaktion mit einem Benutzer dazu führen, dass die Remoteinstallation aufgrund einer Zeitüberschreitung fehlschlägt.

4.2.1 Anforderungen

Grundvoraussetzung für die Remoteinstallation ist ein korrekt konfiguriertes TCP/IP-Netzwerk, das eine zuverlässige Kommunikation zwischen Client und Server ermöglicht. Für die Installation einer Clientlösung auf dem Client-Arbeitsplatzrechner mithilfe von ERA gelten strengere Anforderungen als für eine direkte Installation. Für eine Remoteinstallation müssen die folgenden Voraussetzungen gegeben sein:

- Client für Microsoft-Netzwerke ist aktiviert
- Dienst für die Datei- und Druckerfreigabe ist aktiviert
- Zugriff auf die Ports für die Dateifreigabe (445, 135-139) ist möglich
- TCP/IP ist aktiviert
- Administrative Freigabe ADMIN$ ist aktiviert
- Client reagiert auf PING-Anforderungen
- Verbindung mit ERAS und ERAC ist möglich (Ports 2221- 2224 sind geöffnet)
- Name und Passwort eines Benutzers mit Administratorrechten für die Client-Arbeitsplatzrechner ist vorhanden (Benutzername darf nicht leer sein)
- Einfache Dateifreigabe ist deaktiviert
- Serverdienst ist aktiviert
- Dienst „Remoteregistrierung" ist aktiviert

HINWEIS: In neueren Microsoft Windows-Versionen (Windows Vista, Windows Server 2008 und Windows 7) werden die Berechtigungen von lokalen Benutzerkonten durch entsprechende Sicherheitsrichtlinien eingeschränkt. Bestimmte Vorgänge im Netzwerk können über dieses Konto in manchen Fällen daher eventuell nicht ausgeführt werden. Wenn der ERA-Dienst auf Ihrem System unter einem lokalen Benutzerkonto ausgeführt wird, können bei bestimmten Netzwerkkonfigurationen Probleme bei der Push-Installation auftreten (z. B. bei einer Remoteinstallation aus einer Domäne in einer Arbeitsgruppe). Unter Windows Vista, Windows Server 2008 und Windows 7 empfiehlt es sich daher, den ERA-Dienst unter einem Konto mit ausreichenden Zugriffsrechten für das Netzwerk auszuführen. Um festzulegen, unter welchem Benutzerkonto ERA ausgeführt wird, klicken Sie auf **Start** ' **Systemsteuerung** ' **Verwaltung** ' **Dienste**. Wählen Sie den Dienst ESET Remote Administrator Server in der Liste aus und klicken Sie auf die Registerkarte **Anmelden**. Bei der Installation von ESET Remote Administrator 4 können Sie diese Einstellung nur festlegen, wenn Sie die Installationsart **Benutzerdefiniert (alle Einstellungen anpassbar)** wählen. Stellen Sie bei einer Push-Installation auf Arbeitsplatzrechnern mit Windows Vista, Windows Server 2008 oder Windows 7 sicher, dass sich sowohl Ihr ERA Server als auch die Arbeitsplatzrechner Mitglieder einer Domäne sind.

Es wird dringend empfohlen, vor der Installation alle Voraussetzungen zu überprüfen, insbesondere wenn das Netzwerk eine größere Zahl von Arbeitsplatzrechnern enthält. Wählen Sie hierzu auf der Registerkarte **Remoteinstallation** die Registerkarte **Computer**, klicken Sie mit der rechten Maustaste auf die gewünschten Clients und wählen Sie **Diagnose vor Push-Installation** aus dem Kontextmenü.

4.2.2 Konfigurieren der Umgebung für die Remoteinstallation

Vor der Installation von ESET Security-Produkten auf Computern im Netzwerk sollten Sie als Administrator die Umgebung entsprechend vorbereiten, um Fehler bei der Installation zu vermeiden.

Der Bereich **Netzwerkansicht** der Registerkarte **Remoteinstallation** zeigt eine anpassbare Ansicht des Netzwerks. Hier finden Sie zwei unterschiedliche Anzeigeoptionen.

Konsole

Die Ansicht **Konsole** zeigt das Ergebnis einer normalen NetBIOS-Suche von dem Computer aus, auf dem ERAC installiert ist. Sie zeigt alle verfügbaren Domänen und Arbeitsgruppen. Durch (De-)Aktivieren der dazugehörigen Kontrollkästchen können Sie die Anzeige filtern.

Server

Die Ansicht **Server** bietet Ihnen zusätzliche Filteroptionen. Neben der NetBIOS-Suche können Sie sich hier auch die Computer im Active Directory sowie die vorhandenen ERA-Clients anzeigen lassen oder eigene benutzerdefinierte Filter erstellen.

Für benutzerdefinierte Filter haben Sie zwei Optionen: **Benutzerdefinierte Liste** und **IP-Suche**. Mit beiden können Sie von Hand eigene Gruppen erstellen.
Bei der Option **Benutzerdefinierte Liste** fügen Sie der Gruppe Computer hinzu, indem Sie deren Namen entweder von Hand im Bereich **In der Gruppe enthaltene Computer** eintragen oder aus einer *.txt*-Datei importieren. In beiden Fällen müssen Sie die Computernamen einzeln in Listenform angeben.

Bei der Option **IP-Suche** können Sie IP-Bereiche für Computer sowie Gruppen solcher Bereiche erstellen. Der IP-Bereich dient dann als Filterkriterium.

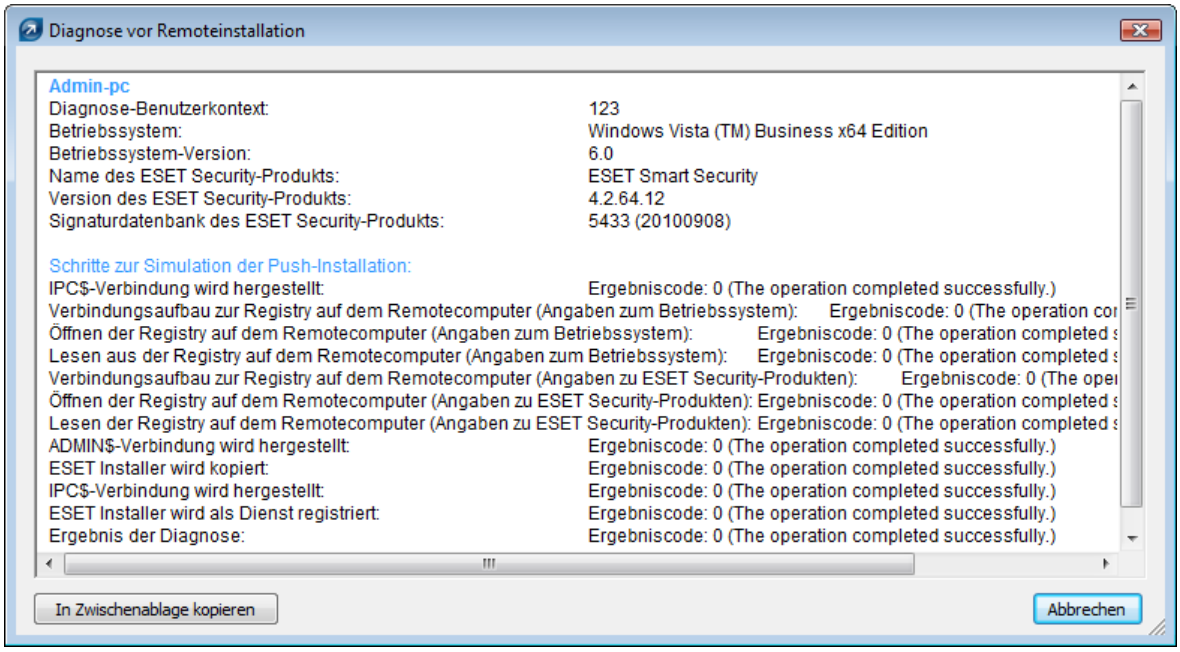
HINWEIS: Die Suchergebnisse im Zweig „Konsole" werden über eine Suche von ERAC aus ermittelt, die Ergebnisse im Zweig „Server" hingegen über eine Suche von ERAS aus. Beachten Sie diesen Unterschied, wenn Sie die Verbindung zu ERAS aus einem anderen Netzwerk aufbauen.

Im Bereich **Filteroptionen** haben Sie zwei weitere Filteroptionen:

Nicht registrierte Computer - Es werden die Computer angezeigt, die nicht in der aktuellen Serverdatenbank aufgeführt sind.

Clients mit Warnung wegen überfälliger Verbindung - Es werden die Computer angezeigt, die in der aktuellen Serverdatenbank aufgeführt sind und für die eine Warnung wegen überfälliger Verbindung vorliegt.

Nachdem Sie die gewünschten Kriterien unter **Netzwerkansicht** und **Filteroptionen** eingerichtet haben, sehen Sie im rechten Teil des Fensters auf der Registerkarte **Computer** eine Liste der Arbeitsplatzrechner, die zur Installation einer Clientlösung geeignet sind. Vor einer Push-Installation auf den angezeigten Computern können Sie eine Diagnose der Voraussetzungen durchführen. Hierzu klicken Sie mit der rechten Maustaste auf die ausgewählten Computer und wählen **Diagnose vor Push-Installation** aus dem Kontextmenü. Auf diese Weise können Sie herausfinden, ob die Voraussetzungen für die Installation erfüllt sind, und mögliche Probleme im Vorfeld erkennen.


Diagnose vor Remoteinstallation
Admin-pc
Diagnose-Benutzerkontext: 123
Betriebssystem: Windows Vista (TM) Business x64 Edition
Betriebssystem-Version: 6.0
Name des ESET Security-Produkts: ESET Smart Security
Version des ESET Security-Produkts: 4.2.64.12
Signaturdatenbank des ESET Security-Produkts: 5433 (20100908)
Schritte zur Simulation der Push-Installation:
IPC$-Verbindung wird hergestellt: Ergebniscode: 0 (The operation completed successfully.)
Verbindungsaufbau zur Registry auf dem Remotecomputer (Angaben zum Betriebssystem): Ergebniscode: 0 (The operation cor
Öffnen der Registry auf dem Remotecomputer (Angaben zum Betriebssystem): Ergebniscode: 0 (The operation completed s
Lesen aus der Registry auf dem Remotecomputer (Angaben zum Betriebssystem): Ergebniscode: 0 (The operation completed s
Verbindungsaufbau zur Registry auf dem Remotecomputer (Angaben zu ESET Security-Produkten): Ergebniscode: 0 (The oper
Öffnen der Registry auf dem Remotecomputer (Angaben zu ESET Security-Produkten): Ergebniscode: 0 (The operation completed s
Lesen der Registry auf dem Remotecomputer (Angaben zu ESET Security-Produkten): Ergebniscode: 0 (The operation completed s
ADMIN$-Verbindung wird hergestellt: Ergebniscode: 0 (The operation completed successfully.)
ESET Installer wird kopiert: Ergebniscode: 0 (The operation completed successfully.)
IPC$-Verbindung wird hergestellt: Ergebniscode: 0 (The operation completed successfully.)
ESET Installer wird als Dienst registriert: Ergebniscode: 0 (The operation completed successfully.)
Ergebnis der Diagnose: Ergebniscode: 0 (The operation completed successfully.)
In Zwischenablage kopieren
Abbrechen

4.2.3 Push-Remoteinstallation

Bei dieser Methode der Remoteinstallation werden die Clientlösungen im Push-Verfahren auf den Zielrechnern installiert. Hierzu müssen die Zielrechner online sein. Sofern diese Voraussetzung gegeben ist, ist die Push-Installation die effektivste Installationsmethode. Bevor Sie eine Push-Installation durchführen können, müssen Sie zunächst die .msi-Installationsdateien für ESET Smart Security bzw. ESET NOD32 Antivirus von der ESET-Website herunterladen und ein Installationspaket erstellen. Zusätzlich können Sie eine Konfigurationsdatei erstellen, die beim Ausführen des Installationspakets automatisch übergeben wird. Beachten Sie vor der Installation bitte auch die Hinweise im Kapitel Anforderungen 39.

Um eine Push-Installation zu starten, gehen Sie wie folgt vor:

1) Stellen Sie sicher, dass die Zielrechner für die Remoteinstallation auf der Registerkarte **Computer** aufgeführt sind. Erstellen Sie dann einen Remoteinstallations-Task, indem Sie mit der rechten Maustaste auf einen oder mehrere dieser Computer klicken und im Kontextmenü **Push-Installation** wählen.

2) Richten Sie die Anmeldedaten für die Computer in der Liste ein (**Festlegen**, **Für alle festlegen**). Das verwendete Konto muss Administratorrechte besitzen. In diesem Schritt können Sie über die Schaltfläche **Clients hinzufügen (mit Auswahlhilfe)** außerdem noch weitere Clients in die Liste aufnehmen.

3) Wählen Sie das Installationspaket aus, das auf den Zielrechnern installiert werden soll.

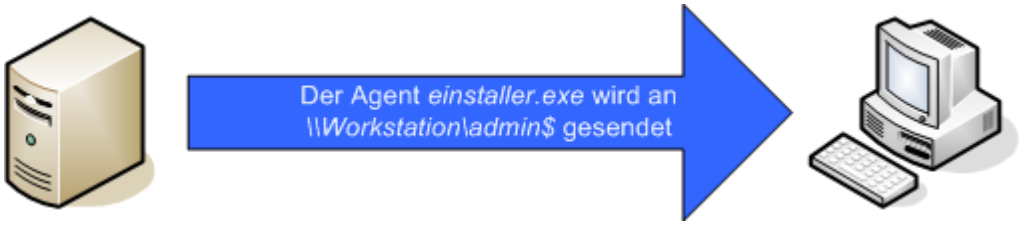
4) Geben Sie an, wann der Task ausgeführt werden soll, und klicken Sie auf **Fertig stellen**.

Auf der Registerkarte **Installations-Tasks** können Sie den Status des Remoteinstallations-Tasks einsehen. Für nähere Informationen zu den Ergebnissen der Diagnose wählen Sie den gewünschten Task aus und drücken F4. Das Dialogfenster **Eigenschaften** wird angezeigt. Auf der Registerkarte **Details** können Sie nun die Ergebnisse der Diagnose für die Remoteinstallation einsehen, indem Sie auf **Alle Logs anzeigen/Ausgewählte Logs anzeigen** klicken.

HINWEIS: Maximal können standardmäßig 20 Remoteinstallations-Threads gleichzeitig ausgeführt werden. Wenn Sie einen Remoteinstallations-Task für eine größere Anzahl von Computern absenden, werden die überzähligen Computer in eine Warteschlange eingereiht und abgearbeitet, sobald wieder Threads frei werden. Aus Leistungsgründen sollte die maximale Threadanzahl möglichst nicht erhöht werden. Sollten Sie dies jedoch trotzdem wünschen, haben Sie im Konfigurationseditor die Möglichkeit dazu (**ESET Remote Administrator** > **ERA Server** > **Einstellungen** > **Remoteinstallation**).

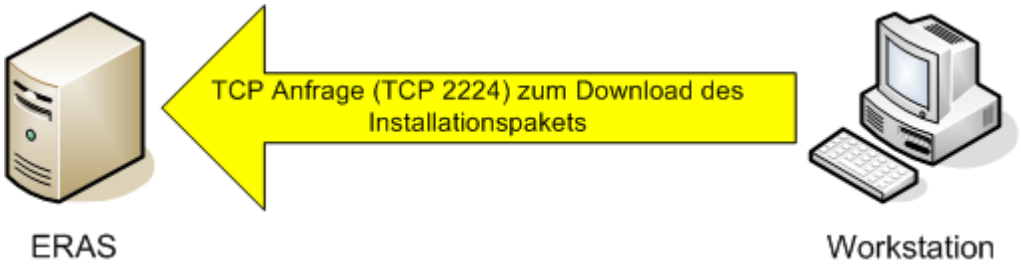
Der weitere Ablauf der Remoteinstallation gestaltet sich wie folgt:

5) ERAS sendet den Agenten *einstaller.exe* über die administrative Freigabe admin$ an den Zielrechner.

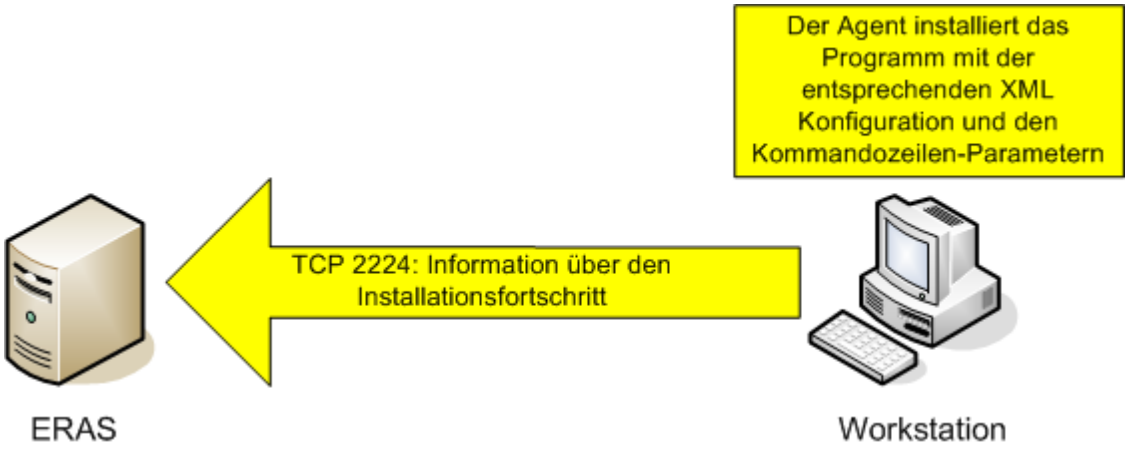


6) Der Agent wird über das Systemkonto als Dienst gestartet.

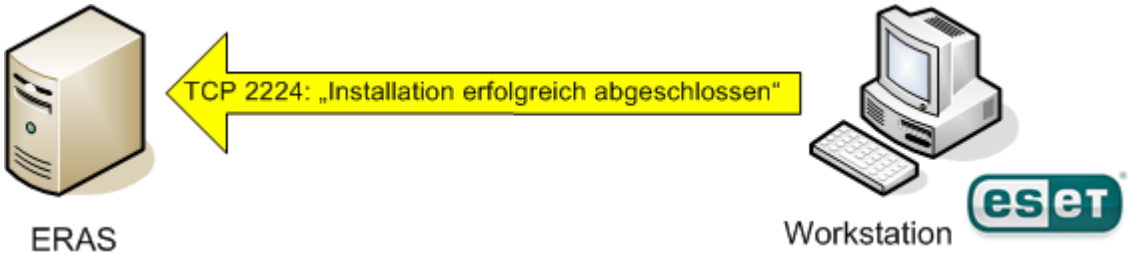
7) Der Agent baut über den TCP-Port 2224 eine Verbindung zu dem ERAS auf, von dem er übermittelt wurde, und lädt das jeweilige Installationspaket herunter.



8) Der Agent installiert das Paket über das in Schritt 2 festgelegte Administratorkonto. Dabei werden eine eventuell vorhandene *.xml*-Konfigurationsdatei sowie die festgelegten Befehlszeilenparameter berücksichtigt.


Der Agent installiert das Programm mit der entsprechenden XML Konfiguration und den Kommandozeilen-Parametern
TCP 2224: Information über den Installationsfortschritt
ERAS
Workstation

9) Direkt nach Abschluss der Installation sendet der Agent eine Nachricht zurück an ERAS. Bei einigen ESET Security-Produkten ist ein Neustart erforderlich. Hierzu erfolgt bei Bedarf eine gesonderte Abfrage.



Im Kontextmenü der Registerkarte **Computer** (Aufruf per Rechtsklick) stehen die folgenden Optionen zur Verfügung:

- **Pakete verwalten**
  Öffnet den **Installationspaket-Editor**. Nähere Informationen finden Sie unter Remoteinstallation 36.
- **Clientupgrade**
  Startet einen Upgrade-Task. Verwenden Sie diese Option, wenn Sie eine neuere Version von ESS/EAV über die ältere Version installieren möchten.
- **Diagnose vor Push-Installation**
  Überprüft, ob die betreffenden Clients sowie die zur Remoteinstallation erforderlichen Dienste verfügbar sind. Nähere Informationen finden Sie im Kapitel Konfigurieren der Umgebung für die Remoteinstallation 39.
- **Push-Installation**
  Startet den Remoteinstallations-Task.
- **In Ordner oder Anmeldeskript exportieren**
  Nähere Informationen finden Sie unter Remoteinstallation per Anmeldeskript/E-Mail 43.
- **Per E-Mail versenden**
  Nähere Informationen finden Sie unter Remoteinstallation per Anmeldeskript/E-Mail 43.
- **Standard-Anmeldedaten für Installation per E-Mail oder Anmeldeskript festlegen**
  Öffnet das Dialogfenster **Standardanmeldung**, wo Sie den Benutzernamen und das Passwort eines Kontos mit Administratorrechten auf den Zielrechnern angeben können.
- **Eigenschaften**
  Öffnet das Dialogfenster **Eigenschaften** mit allen wichtigen Informationen zum betreffenden Client.

Informationen zu den anderen Optionen im Kontextmenü finden Sie im Kapitel Kontextmenü 22.

4.2.4 Remoteinstallation per Anmeldeskript/E-Mail

Die Remoteinstallation per Anmeldeskript und die Remoteinstallation per E-Mail ähneln sich in vielerlei Hinsicht. Der einzige Unterschied liegt in der Art, wie der Agent *einstaller.exe* auf die Client-Arbeitsplatzrechner übertragen wird. Dies kann bei ERA entweder über ein Anmeldeskript oder per E-Mail geschehen. Der Agent *einstaller.exe* kann auch als Standalone-Programm verwendet und auf anderem Wege ausgeführt werden (siehe hierzu das Kapitel Benutzerdefinierte Remoteinstallation 45).
Die Installation per Anmeldeskript eignet sich gut für Notebooks, die oft außerhalb des lokalen Netzwerks verwendet werden. In diesem Fall findet die Installation statt, sobald sich der Benutzer an der Domäne anmeldet. Für Geräte dieses Typs ist die Remoteinstallation per Anmeldeskript die empfohlene Methode.

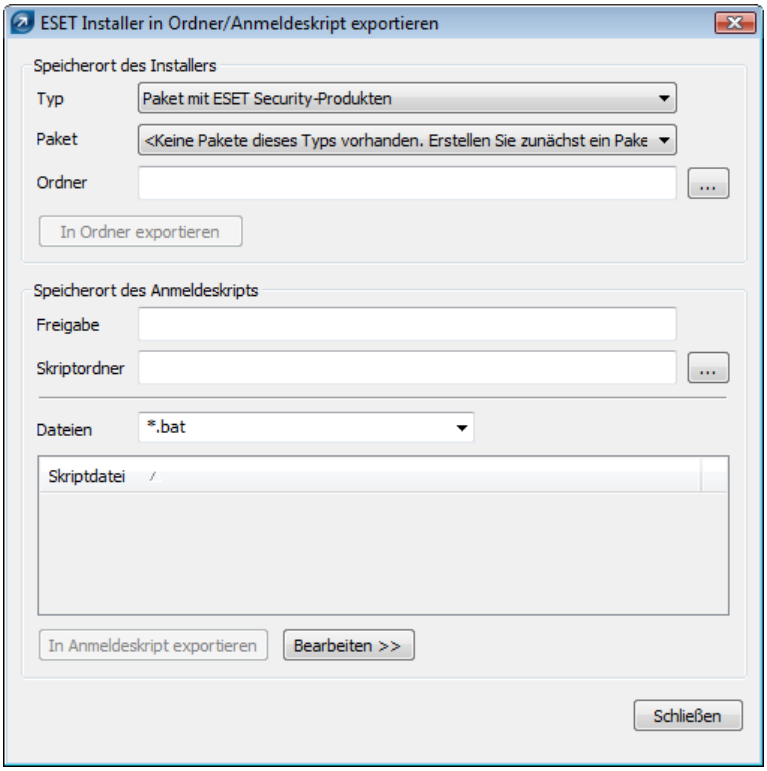
Während das Anmeldeskript automatisch beim Anmelden des Benutzers gestartet wird, ist für die Remoteinstallation per E-Mail ein Benutzereingriff nötig. Hier muss der Benutzer den Agenten einstaller.exe aus der E-Mail-Anlage ausführen. Bei wiederholten Aufrufen wird keine erneute Installation der jeweiligen ESET Clientsoftware gestartet. Nähere Informationen finden Sie im Kapitel Vermeiden wiederholter Installationen 46.

Der Aufruf des Agenten *einstaller.exe* kann über einen normalen Texteditor oder ein proprietäres Werkzeug ins Anmeldeskript eingefügt werden. Auch der Versand der Datei *einstaller.exe* als E-Mail-Anlage kann über ein beliebiges E-Mail-Programm erfolgen. Unabhängig von der verwendeten Methode müssen Sie sicherstellen, dass Sie die korrekte *einstaller.exe*-Datei verwenden.

Zum Start von *einstaller.exe* muss der aktuell angemeldete Benutzer nicht unbedingt über Administratorrechte verfügen. Der Agent übernimmt die erforderlichen Administrator-Anmeldedaten (Benutzer/Passwort/Domäne) aus ERAS. Nähere Informationen finden Sie am Ende dieses Kapitels.

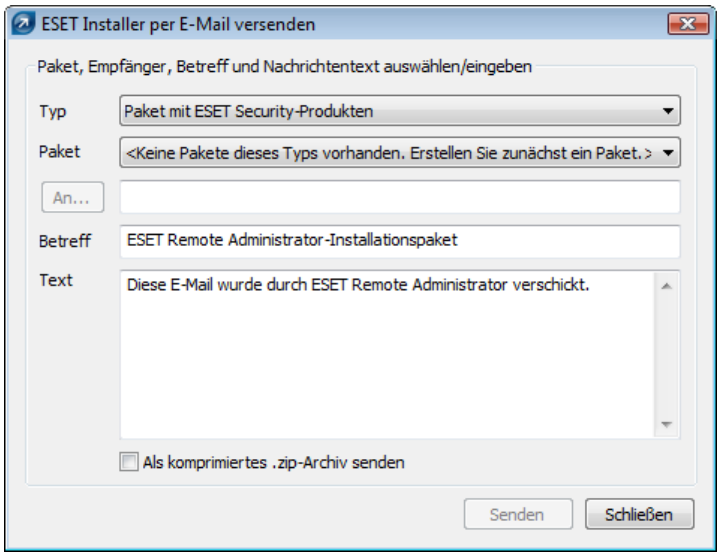
Um den Aufruf von *einstaller.exe* in ein Anmeldeskript einzufügen, gehen Sie wie folgt vor:

1) Klicken Sie mit der rechten Maustaste auf die Registerkarte **Remoteinstallation** und wählen Sie **In Ordner oder Anmeldeskript exportieren**. Wählen Sie dann **Typ** und Name des zu installierenden **Pakets**.
2) Klicken Sie neben **Ordner** auf die Durchsuchen-Schaltfläche (...) und wählen Sie das Verzeichnis aus, in dem die Datei *einstaller.exe* im Netzwerk bereitgestellt wird. Klicken Sie auf **OK**.
3) Überprüfen Sie die Pfadangabe im Feld **Freigabe** und ändern Sie sie gegebenenfalls.
4) Klicken Sie neben **Skriptordner** auf **...** und wählen Sie den Ordner aus, in dem das Skript gespeichert ist. Passen Sie ggf. die Anzeigemaske an (Feld **Dateien**).
5) Wählen Sie im Bereich **Dateien** die Datei aus, in die die Zeile mit dem Aufruf von *einstaller.exe* eingefügt werden soll.
6) Klicken Sie auf **In Anmeldeskript exportieren**, um die Zeile einzufügen.
7) Um die Position der Zeile zu verändern, klicken Sie auf **Bearbeiten >>**. Zum Speichern klicken Sie auf **Speichern**.

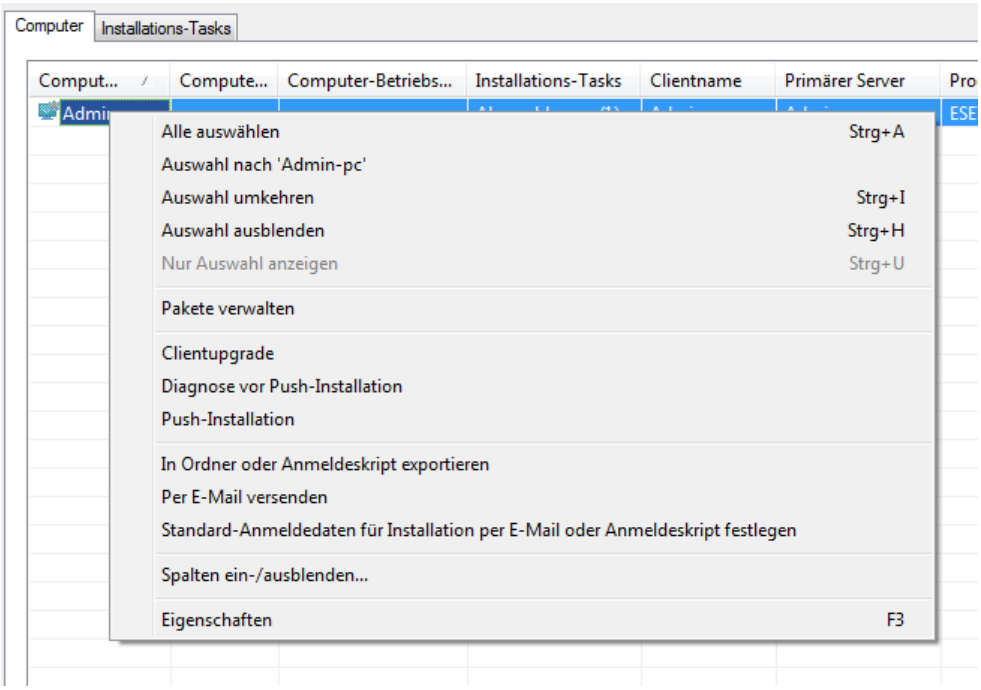


Um den Agenten *einstaller.exe* als E-Mail-Anlage zu verschicken, gehen Sie wie folgt vor:

1) Klicken Sie auf der Registerkarte **Remoteinstallation** auf **Per E-Mail versenden** und wählen Sie **Typ** und Namen des zu installierenden **Pakets** aus.
2) Klicken Sie auf **An**, um E-Mail-Adressen aus dem Adressbuch auszuwählen, oder geben Sie die gewünschten Adressen von Hand ein.
3) Geben Sie im Feld **Betreff** eine Betreffzeile ein.
4) Geben Sie im Feld **Text** eine Nachricht ein.
5) Wenn der Agent als komprimiertes .zip-Archiv verschickt werden soll, aktivieren Sie die Option **Als komprimiertes .zip-Archiv senden**.
6) Klicken Sie auf **Senden**, um die Nachricht abzuschicken.



Während der Remoteinstallation wird vom Zielrechner aus eine Verbindung zu ERAS aufgebaut, und der Agent (*einstaller.exe*) übernimmt die Anmeldedaten, die Sie über den Befehl **Standard-Anmeldedaten für Installation per E-Mail oder Anmeldeskript festlegen** im Kontextmenü festgelegt haben.



Das zur Installation des Pakets verwendete Benutzerkonto muss ein Administratorkonto sein oder besser noch über Domänenadministrator-Rechte verfügen. Die im Dialogfenster **Standardanmeldung** eingegebenen Werte bleiben nur bis zum nächsten Neustart des Serverdienstes (ERAS) gespeichert.

4.2.5 Benutzerdefinierte Remoteinstallation

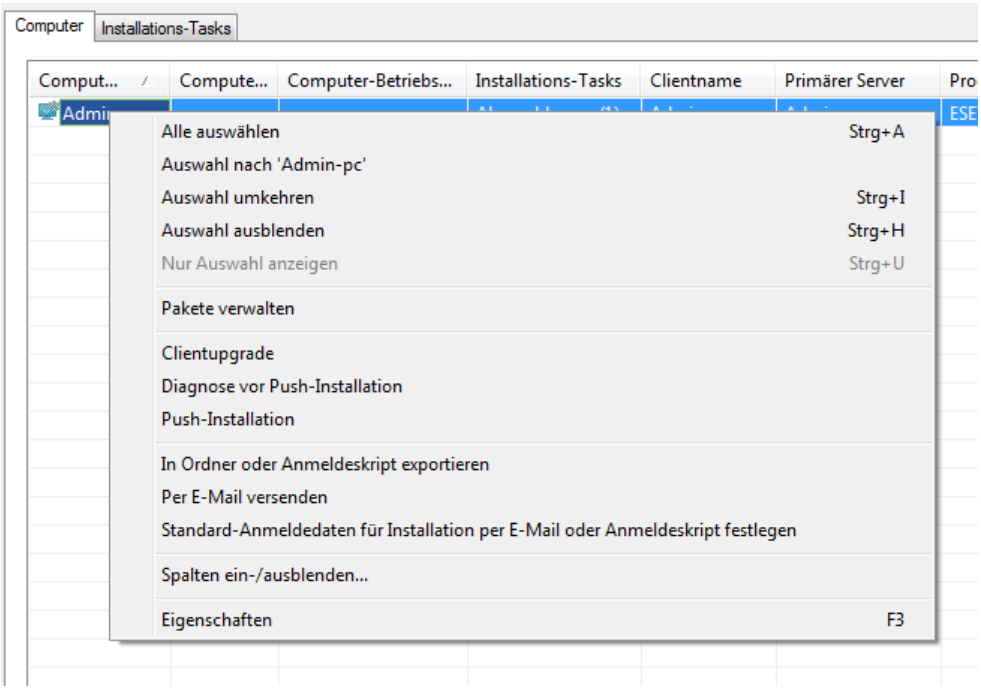
Eine Remoteinstallation von ESET Clientlösungen muss nicht unbedingt über die entsprechenden Funktionen von ERA erfolgen. Letztendlich muss im Wesentlichen nur ein Weg gefunden werden, die Datei *einstaller.exe* auf die Client-Arbeitsplatzrechner zu übertragen und sie dort auszuführen.

Zum Start von *einstaller.exe* muss der aktuell angemeldete Benutzer nicht unbedingt über Administratorrechte verfügen. Der Agent übernimmt die erforderlichen Administrator-Anmeldedaten (Benutzer/Passwort/Domäne) aus ERAS. Nähere Informationen finden Sie am Ende dieses Kapitels.

Um die Datei *einstaller.exe* zu erhalten, gehen Sie wie folgt vor:

- Aktivieren Sie auf der Registerkarte **Remoteinstallation** die Registerkarte **Computer**. Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle, wählen Sie im Kontextmenü den Befehl **In Ordner oder Anmeldeskript exportieren** und wählen Sie **Typ** und Namen des zu installierenden **Pakets**.
- Klicken Sie neben **Ordner** auf **...** und wählen Sie das Verzeichnis aus, in das Sie die Datei *einstaller.exe* exportieren möchten.
- Klicken Sie auf **In Ordner exportieren**.
- Die extrahierte Datei *einstaller.exe* können Sie nun je nach Wunsch weiterverwenden.

HINWEIS: Wenn ein Benutzerkonto mit Administratorrechten für die Installation bereitsteht, kann die Methode *„Direkte Installation mit vordefinierter XML-Konfiguration"* verwendet werden. Das *.msi*-Paket wird dabei mit dem Parameter */qn* (Versionen 4.x, 3.x) bzw. */silentmode* (Version 2.x) gestartet. Hierdurch wird die Installation im unbeaufsichtigten Modus ohne Benutzeroberfläche durchgeführt.



Das zur Installation des Pakets verwendete Benutzerkonto muss ein Administratorkonto sein oder besser noch über Domänenadministrator-Rechte verfügen.

Während der Remoteinstallation wird vom Zielrechner aus eine Verbindung zu ERAS aufgebaut, und der Agent (*einstaller.exe*) übernimmt die Anmeldedaten, die Sie über den Befehl **Standard-Anmeldedaten für Installation per E-Mail oder Anmeldeskript festlegen** festgelegt haben.

Wird der Agent *einstaller.exe* manuell auf dem Zielrechner gestartet, läuft die Remoteinstallation wie folgt ab:

- Der Agent *einstaller.exe* sendet eine Anforderung an ERAS (TCP-Port 2224).
- ERAS startet mit einem neuen Agenten eine neue Push-Installation des betreffenden Pakets, wobei dieses zunächst über die administrative Freigabe *admin$* übertragen wird. Der Agent wartet auf eine Antwort von ERAS, dass das Paket über die Freigabe *admin$* übertragen wird. Falls keine Antwort erfolgt, versucht der Agent, das Installationspaket über den TCP/IP-Port 2224 herunterzuladen. In diesem Fall werden die in ERAS über **Remoteinstallation > Anmeldung** festgelegten Administrator-Anmeldedaten nicht übertragen. Der Agent versucht dann, das Paket über das aktuelle Benutzerkonto zu installieren. Unter Microsoft Windows 9x/Me kann die

administrative Freigabe nicht verwendet werden. Der Agent baut in diesem Fall automatisch eine direkte TCP/IP-Verbindung zum Server auf. Anschließend lädt er das Paket per TCP/IP von ERAS herunter.

Die Installation des Pakets wird gestartet, wobei die per .xml-Datei festgelegten Parameter und das in ERAS definierte Benutzerkonto (**Standard-Anmeldedaten für Installation per E-Mail oder Anmeldeskript festlegen**) verwendet werden.

4.2.6 Upgrade

Diese Installationsart ist für Clients mit ESS/EAV ab der Version 4.2 gedacht. Ab dieser Version ist ein neuer Upgrade-Mechanismus vorhanden, über den ERA ein Clientupgrade einleiten kann, ohne dass dafür der Agent *einstaller.exe* erforderlich ist. Dies funktioniert ähnlich wie bei einem Programmkomponenten-Update (PCU), mit dem Clients auf eine neuere Programmversion aktualisiert werden. Für ESS-/EAV-Clients ab der Version 4.2 wird diese Upgrade-Methode dringend empfohlen.

HINWEIS: Eine eventuell vorhandene benutzerdefinierte Konfigurationsdatei im Installationspaket wird beim Upgrade ignoriert.

4.2.7 Vermeiden wiederholter Installationen

Direkt nach dem erfolgreichen Abschluss der Remoteinstallation setzt der Agent auf dem Remoteclient eine Markierung, die verhindert, dass dasselbe Installationspaket erneut installiert wird. Die Markierung wird in den folgenden Registrierungsschlüssel geschrieben:

HKEY_LOCAL_MACHINE\Software\ESET\ESET Remote Installer

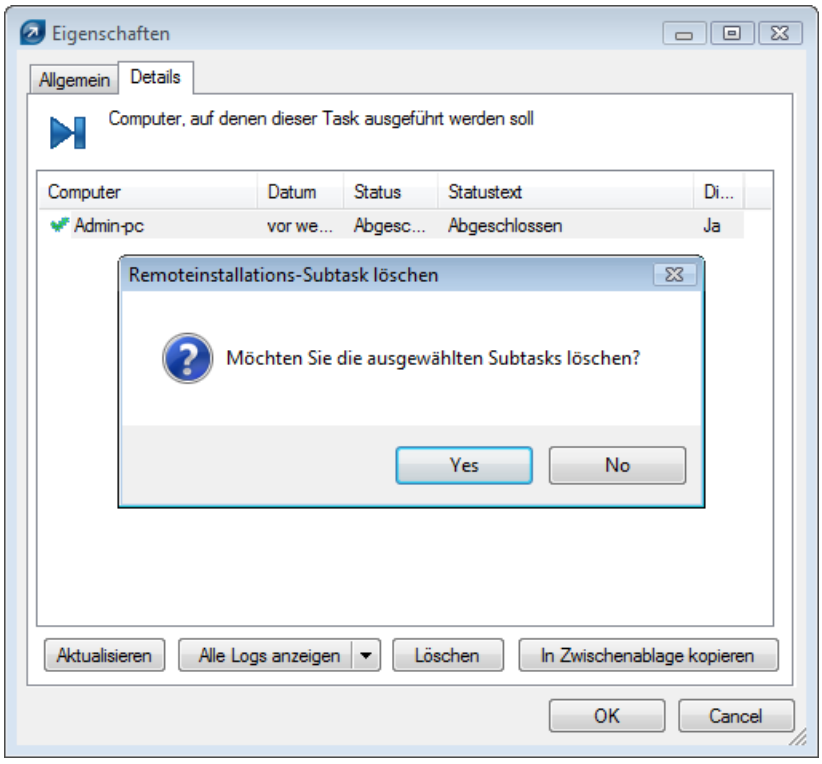
Wenn bei einem erneuten Aufruf des Agenten *einstaller.exe* der angegebene Typ und Name des Pakets mit den in der Registrierungsdatenbank hinterlegten Daten übereinstimmen, wird die Installation nicht durchgeführt. So wird verhindert, dass die Software bei wiederholten Installationen immer wieder neu auf demselben Rechner installiert wird.

HINWEIS: Bei der Push-Remoteinstallation wird dieser Registrierungsschlüssel ignoriert.

ERAS bietet eine weitere Funktion, um wiederholte Installationen zu verhindern: Sobald der Agent über den TCP-Port 2224 die Rückverbindung zum ERAS aufbaut, findet eine Prüfung statt. Falls für den Zielrechner eine Fehlermeldung vorliegt oder die Installation bereits erfolgreich abgeschlossen wurde, werden weitere Installationsversuche unterbunden.

Der Agent schreibt dann den folgenden Fehler in das Installationsprotokoll *%TEMP%\einstaller.log*:

ESET Installer auf Anforderung des Servers '%s:%d' beendet.



Wenn wiederholte Installationen nicht von ERAS unterbunden werden sollen, müssen Sie die entsprechenden Einträge auf der Registerkarte **Details** im Eigenschaften-Dialogfeld des Remoteinstallations-Tasks entfernen. Um einen Eintrag zu entfernen, wählen Sie ihn aus, klicken auf **Löschen** und bestätigen mit **Ja**.

4.3 Installation in einer großen Unternehmensumgebung

Bei der Bereitstellung von Programmen in großen Netzwerken muss ein Tool zum Einsatz kommen, das eine Remoteinstallation der Programme auf jedem einzelnen Zielrechner gewährleisten kann.

Installation per Gruppenrichtlinie

In einer Active Directory-Umgebung lässt sich diese Aufgabe elegant über eine Installation per Gruppenrichtlinie lösen. Die Installation findet hierbei über ein Installationspaket statt, das über die Gruppenrichtlinie direkt an alle Clients in der Domäne verteilt wird.

Um einen Domänencontroller so zu konfigurieren, dass ESET Smart Security bzw. ESET NOD32 Antivirus auf jedem Arbeitsplatzrechner automatisch nach dem Anmelden installiert wird, gehen Sie wie folgt vor:

1) Erstellen Sie einen freigegebenen Ordner auf den Domänencontroller. Alle Arbeitsplatzrechner müssen über Leserechte für diesen Ordner verfügen.

2) Kopieren Sie das Installationspaket (*.msi*-Datei) für ESET Smart Security bzw. ESET NOD32 Antivirus in diesen Ordner.

3) Speichern Sie im gleichen Ordner eine *.xml*-Konfigurationsdatei mit der gewünschten Konfiguration für das Programm. Die Datei sollte den Namen *cfg.xml* tragen. Zum Erstellen der Konfigurationsdatei können Sie den ESET Configuration Editor verwenden. Nähere Informationen finden Sie im Kapitel ESET Configuration Editor 32.

4) Klicken Sie auf **Start** > **Programme** > **Verwaltung** > **Active Directory-Benutzer und -Computer**.

5) Klicken Sie mit der rechten Maustaste auf den Domänennamen und wählen Sie **Eigenschaften** > **Gruppenrichtlinie** > **Bearbeiten** > **Benutzerkonfiguration**.

6) Klicken Sie mit der rechten Maustaste auf **Softwareeinstellungen** und wählen Sie **Neu** > **Paket**.

7) Geben Sie im Dialogfenster **Öffnen** den UNC-Pfad zum Installationspaket auf der Freigabe an (*Computername**Pfad**Installationspaket.msi*) und klicken Sie auf **Öffnen**. Wählen Sie das Installationspaket nicht über die Option **Durchsuchen** aus, da diese nicht den erforderlichen UNC-Pfad, sondern einen lokalen Netzwerkpfad zurückgibt.

8) Aktivieren Sie im nächsten Dialogfenster die Option **Zugewiesen**. Klicken Sie dann auf **OK**, um das Fenster zu schließen.

Mit diesen Schritten wird das Installationspaket auf jedem Computer installiert, der sich an der Domäne anmeldet. Zur Installation des Pakets auf bereits laufenden Rechnern müssen sich die betreffenden Benutzer ab- und dann wieder anmelden.

Wenn die Benutzer selbst entscheiden sollen, ob sie das Paket installieren möchten, wählen Sie in Schritt 8 nicht **Zugewiesen**, sondern **Veröffentlichen**. Bei der nächsten Anmeldung des Benutzers wird das Paket unter **Systemsteuerung** > **Software** > **Neue Programme hinzufügen** > **Programme aus dem Netzwerk hinzufügen** hinzugefügt. Dort steht es dann zur späteren Installation zur Verfügung.

5. Verwalten der Clientcomputer

5.1 Tasks

Sobald Client-Arbeitsplatzrechner eine funktionierende Verbindung zu ERAS aufgebaut haben und in ERAC angezeigt werden, können Sie sie mithilfe von Tasks auf verschiedene Weise konfigurieren und administrieren.

Der unten beschriebene Ablauf gilt für alle Typen von Tasks, die in den nachfolgenden Unterkapiteln beschrieben werden. Die einzige Ausnahme ist der Tasktyp Interaktiver Task 52; nähere Informationen zum diesbezüglichen Arbeitsablauf finden Sie im dazugehörigen Kapitel.

Schritt 1 - **Neuer Task**
Sie können Tasks auf mehreren einzeln ausgewählten Clients oder auf allen Clients aus einer oder mehreren Gruppen ausführen.

1) Um Clients einzeln auszuwählen, wählen Sie sie auf der Registerkarte **Clients** aus und klicken mit der rechten Maustaste darauf.

2) Klicken Sie auf **Neuer Task** und wählen Sie dann den gewünschten Tasktyp.

   HINWEIS: Sie können den Task-Assistenten alternativ auch über den Punkt **Aktionen > Neuer Task** im ERAC-Hauptmenü öffnen.

Schritt 2 - Auswahl des Tasktyps:

Konfigurations-Task 49
On-Demand-Scan (ohne Säubern) 49
On-Demand-Scan (mit Säubern) 49
Update starten 50
SysInspector-Skript-Task 50
Aus Quarantäne wiederherstellen/löschen 51
Sicherheits-Auditlog erzeugen 51
Hinweis anzeigen 51

3) Nachdem Sie den gewünschten Tasktyp ausgewählt haben, konfigurieren Sie den Task wie im dazugehörigen Kapitel (siehe oben stehende Links) beschrieben.

Schritt 3 - **Clients auswählen**

4) Nach der Konfiguration des Tasks wird das Dialogfenster **Clients auswählen** angezeigt, wo Sie noch einmal die Möglichkeit haben, die Clientauswahl anzupassen. Sie können zusätzliche Clients aus der Liste **Alle Objekte** (links im Fenster) in die Liste **Ausgewählte Objekte** (rechts im Fenster) übernehmen oder vorhandene Clienteinträge entfernen.

   HINWEIS: Über die Schaltfläche **Hinzufügen (erweitert)** können Sie ein zusätzliches Dialogfenster öffnen, in dem Sie Clients aus der Registerkarte **Clients** bzw. nach ihrem **Server** und/oder ihrer **Gruppe** auswählen können.

Schritt 4 - **Taskbericht, Fertig stellen**

5) Im letzten Dialogfenster **Taskbericht** wird die Task-Konfiguration noch einmal zusammengefasst. Wahlweise können Sie noch einen Namen und eine Beschreibung für den Task eingeben. Über die Option **Task ausführen ab** können Sie festlegen, dass der Task erst ab einem bestimmten Zeitpunkt ausgeführt werden soll. Wenn Sie die Option **Tasks bei erfolgreichem Abschluss automatisch löschen** aktivieren, werden Tasks nach erfolgreicher Übermittlung an die Zielrechner automatisch gelöscht.

6) Klicken Sie auf **Fertig stellen**, um den Task zur Ausführung zu aktivieren.

Die folgenden Unterkapitel beschreiben die einzelnen Tasktypen für Client-Arbeitsplatzrechner und geben ein kurzes Beispielszenario für jeden Typ.

5.1.1 Konfigurations-Task

Konfigurations-Tasks dienen zum Ändern der Schutzeinstellungen auf Client-Arbeitsplatzrechnern. Sie werden in Form eines Konfigurationspakets mit den Änderungsparametern an die Zielrechner übermittelt. Auch *.xml*-Dateien, die im ESET Configuration Editor erstellt oder von Clients exportiert wurden, sind mit Konfigurations-Tasks kompatibel. Das folgende Beispiel zeigt, wie Sie mit einem Konfiguration-Task den Benutzernamen und das Passwort auf den Zielrechnern ändern. Alle Einstellungen und Optionen, die in diesem Beispiel nicht verwendet werden, sind am Ende dieses Kapitels beschrieben.

Zunächst legen Sie fest, an welche Arbeitsplatzrechner der Task übermittelt werden soll. Wählen Sie diese Rechner auf der Registerkarte **Clients** in ERAC aus.

1) Klicken Sie mit der rechten Maustaste auf einen der ausgewählten Rechner und wählen Sie im Kontextmenü **Neuer Task** > **Konfigurations-Task**.

2) Der Assistent **Konfiguration für Clients** wird angezeigt. Hier können Sie über die Schaltflächen **Erstellen**, **Auswählen** sowie **Aus Vorlage erstellen** die zu verwendende Konfigurationsdatei festlegen.

3) Klicken Sie auf **Erstellen**, um den ESET Configuration Editor zu öffnen, und richten Sie die gewünschte Konfiguration ein. Gehen Sie zu den Einträgen **ESET Smart Security/ESET NOD32 Antivirus** > **Update-Modul Profil** > **Einstellungen** > **Benutzername** und **Passwort**.

4) Tragen Sie den von ESET bereitgestellten Benutzernamen und das Passwort ein und klicken Sie rechts auf **Zurück zur Konsole**, um zum Task-Assistenten zurückzukehren. Der Pfad zum Konfigurationspaket erscheint nun unter **Konfiguration erstellen/auswählen**.

5) Wenn Sie bereits eine Konfigurationsdatei mit den gewünschten Änderungen haben, klicken Sie auf **Auswählen** und wählen sie aus. Die Datei wird mit dem Konfigurations-Task verknüpft.

6) Alternativ können Sie auch auf **Aus Vorlage erstellen** klicken, die *.xml*-Datei auswählen und ggf. die gewünschten Änderungen vornehmen.

7) Um die gerade erstellte/bearbeitete Konfigurationsdatei noch einmal einzusehen oder Änderungen daran vorzunehmen, klicken Sie auf **Anzeigen** bzw. **Bearbeiten**.

8) Klicken Sie auf **Weiter**. Das Dialogfeld **Clients auswählen** wird angezeigt. Hier sehen Sie die Arbeitsplatzrechner, an die der Task übermittelt wird. Sie können nun weitere Clients einzeln hinzufügen oder über ihren Server/ihre Gruppe auswählen. Klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

9) Im letzten Dialogfenster **Taskbericht** wird die Task-Konfiguration noch einmal zusammengefasst. Wahlweise können Sie noch einen Namen und eine Beschreibung für den Task eingeben. Über die Option **Task ausführen ab** können Sie festlegen, dass der Task erst ab einem bestimmten Zeitpunkt ausgeführt werden soll. Wenn Sie die Option **Tasks bei erfolgreichem Abschluss automatisch löschen** aktivieren, werden Tasks nach erfolgreicher Übermittlung an die Zielrechner automatisch gelöscht.

10) Klicken Sie auf **Fertig stellen**, um den Task zur Ausführung zu aktivieren.

5.1.2 Task "On-Demand-Scan"

Für einen On-Demand-Scan bietet der Kontextmenü-Befehl **Neuer Task** zwei unterschiedliche Optionen. Mit der ersten Option **On-Demand-Scan (ohne Säubern)** wird beim Scan nur ein Log erzeugt, infizierte Dateien werden jedoch nicht weiter bearbeitet. Die zweite Option ist demgegenüber **On-Demand-Scan (mit Säubern)**.

Das Dialogfenster **On-Demand-Scan** enthält für beide Varianten die gleichen Standardeinstellungen, ausgenommen die Option **Nur prüfen, keine Aktion**. Diese Option legt fest, ob der Scanner infizierte Dateien säubern soll. Das folgende Beispiel illustriert die Erstellung eines Tasks für einen On-Demand-Scan.

1) Über die Liste **Konfigurationsbereich** legen Sie fest, für welches ESET Produkt der Scantask definiert werden soll. Wählen Sie hier die Produkte aus, die auf den Zielrechnern installiert sind.

   HINWEIS: Mit der Option **Diesen Bereich von Task für On-Demand-Scan ausnehmen** werden alle Einstellungen für den unter **Konfigurationsbereich** ausgewählten Produkttyp deaktiviert und kommen auf Clients, auf denen das betreffende Produkt installiert ist, demzufolge nicht zur Anwendung. Alle Clients mit diesem Produkt werden also aus der Empfängerliste entfernt. Wenn Sie als Administrator Clients als Empfänger auswählen, dann aber das dort

installierte Produkt über diese Option ausschließen, schlägt der Task mit einer entsprechenden Meldung fehl. Um dies zu vermeiden, sollten Sie stets passende Clients für den Task auswählen.

2) Unter **Profilname** können Sie ein Scanprofil für den Task auswählen.

3) Wählen Sie im Bereich **Zu prüfende Laufwerke**, welche Arten von Laufwerken auf den Clientcomputern geprüft werden sollen. Wenn Ihnen die Auswahl zu allgemein ist, können Sie auch den exakten Pfad der zu prüfenden Objekte festlegen. Verwenden Sie hierzu das Feld **Pfad** oder die Schaltfläche **Pfad hinzufügen**. Um die ursprüngliche Laufwerksauswahl für den Scan wiederherzustellen, wählen Sie **Verlauf löschen**.

4) Klicken Sie auf **Weiter**, um zu den Dialogfenstern **Clients auswählen** und **Taskbericht** zu gelangen. Diese sind ausführlich im Kapitel Tasks 48 beschrieben.

5) Nach Abschluss des Tasks auf den Clients werden die Ergebnisse an ERAS gemeldet und können in ERAC auf der Registerkarte **Scan-Log** eingesehen werden.

5.1.3 Task "Update starten"

Mit diesem Task können Sie ein Update auf den Zielrechner erzwingen (sowohl der Signaturdatenbank als auch der Programmkomponenten).

1) Klicken Sie auf der Registerkarte **Clients** auf einen beliebigen Rechner und wählen Sie **Neuer Task** > **Update starten**.

2) Wenn Sie bestimmte ESET Security-Produkte vom Update ausnehmen möchten, wählen Sie sie in der Liste **Konfigurationsbereich** aus und aktivieren das Kontrollkästchen **Diesen Bereich vom Update-Task ausnehmen**.

3) Um ein bestimmtes Update-Profil für den Task **Update starten** zu verwenden, aktivieren Sie das Kontrollkästchen **Profilnamen angeben** und wählen das gewünschte Profil aus. Sie können auch die Option **Benutzerdefinierter Profilname** wählen und den Profilnamen von Hand eingeben. Um den Feldwert auf die Standardeinstellung zurückzusetzen, klicken Sie auf **Verlauf löschen**.

4) Klicken Sie auf **Weiter**, um mit den Dialogfenstern **Clients auswählen** und **Taskbericht** fortzufahren. Eine Beschreibung dieser Fenster finden Sie im Kapitel Tasks 48.

5.1.4 SysInspector-Skript-Task

Mit einem SysInspector-Skript-Task können Sie Skripte auf den Zielrechnern ausführen. Auf diese Weise können Sie unerwünschte Objekte vom System entfernen. Nähere Informationen finden Sie auf der Seite ESET SysInspector 100 der Hilfe.

1) Nachdem Sie die Schritte 1 und 2 gemäß der Beschreibung im Kapitel Tasks 48 ausgeführt haben, klicken Sie auf **Auswählen**, um das Skript auszuwählen, das auf dem Zielrechner ausgeführt werden soll.

2) Wenn Sie noch Änderungen am Skript vornehmen möchten, klicken Sie auf **Anzeigen / Bearbeiten**.

3) Klicken Sie auf **Weiter**, um zu den Dialogfenstern **Clients auswählen** und **Taskbericht** zu gelangen. Diese sind ausführlich im Kapitel Tasks 48 beschrieben.

4) Nach Abschluss des Tasks auf dem Client-Arbeitsplatzrechner werden die entsprechenden Informationen in der Spalte **Status** der Registerkarte **Tasks** angezeigt.

HINWEIS: SysInspector-Skript-Tasks werden erst ab ESET Smart Security/ESET NOD32 Antivirus Version 4.0 unterstützt.

5.1.5 Task "Aus Quarantäne wiederherstellen/löschen"

Mit diesem Tasktyp können Sie Quarantäneobjekte gezielt aus der Client-Quarantäne wiederherstellen oder löschen.

1) Nachdem Sie das Dialogfenster **Aus Quarantäne wiederherstellen/löschen** geöffnet haben (siehe dazu das Kapitel Tasks 48), wählen Sie über die Optionsschaltfläche **Wiederherstellen/Löschen** aus, was mit dem Quarantäneobjekt geschehen soll.

   HINWEIS: Wenn Sie ein Objekt aus der Quarantäne wiederherstellen möchten, das weiterhin als Bedrohung erkannt wird, sollten Sie ggf. die Option **Ausschluss hinzufügen** aktivieren. Ansonsten kann es sein, dass der Virenschutz die Aktion unterbindet oder das Objekt erneut in die Quarantäne verschiebt.

2) Wählen Sie eine Bedingung aus, um festzulegen, welche Quarantäneobjekte wiederhergestellt/gelöscht werden sollen, und klicken Sie auf „Weiter".

   HINWEIS: Wenn Sie das Dialogfenster **Aus Quarantäne wiederherstellen/löschen** über das Kontextmenü eines Eintrags auf der Registerkarte **Quarantäne** aufgerufen haben, müssen Sie keine Bedingung angeben. Die Option **Nach Hash** ist dann automatisch ausgewählt, und der Hashwert der Quarantänedatei ist bereits als Kriterium eingetragen.

3) Wählen Sie die Clients für den Wiederherstellung-/Löschvorgang aus (siehe Kapitel Tasks 48) und klicken Sie auf **Weiter**.

4) Das Dialogfenster **Taskbericht** wird angezeigt. Überprüfen Sie noch einmal die Einstellungen, geben Sie dem Task einen Namen, legen Sie ggf. den Ausführungszeitpunkt und die Löschoptionen fest und klicken Sie zum Abschluss auf **Fertig stellen**, um den Task zu bestätigen. Nähere Informationen finden Sie im Kapitel Tasks 48.

5.1.6 Task "Sicherheits-Auditlog erzeugen"

Dieser Tasktyp ist nur für ESET Mobile Security relevant.

Der Sicherheits-Audit umfasst die folgenden Informationen: Akkuladestand, Bluetooth-Status, freier Speicherplatz auf dem Datenträger, Sichtbarkeit des Geräts, Stammnetz und laufende Prozesse. Es wird ein ausführlicher Bericht erzeugt, aus dem unter anderem hervorgeht, ob eine der Angaben unter einem festgelegten Grenzwert liegt oder ein mögliches Sicherheitsrisiko darstellt (z. B. Sichtbarkeit des Geräts aktiviert usw.).

So starten Sie einen Sicherheits-Audit auf dem Mobiltelefon:
1. Klicken Sie auf der Registerkarte **Clients** mit der rechten Maustaste auf den Namen des Clients und wählen Sie im Kontextmenü **Neuer Task** > **Sicherheits-Auditlog erzeugen**.
2. Klicken Sie auf **Weiter**, um mit den Dialogfenstern **Clients auswählen** und **Taskbericht** fortzufahren. Eine Beschreibung dieser Fenster finden Sie im Kapitel Tasks 48.

5.1.7 Task "Hinweis anzeigen"

Dieser Tasktyp ist nur für ESET Mobile Security relevant.

Um einen Hinweis (z. B. eine Warnmeldung) auf dem Mobiltelefon anzuzeigen, gehen Sie wie folgt vor:
1. Klicken Sie auf der Registerkarte **Clients** mit der rechten Maustaste auf den Namen des Clients und wählen Sie im Kontextmenü **Neuer Task** > **Hinweis anzeigen**.
2. Geben Sie **Überschrift** und **Text** für den Hinweis in den entsprechenden Feldern ein und legen Sie die Einstellung **Inhalt** fest.
3. Klicken Sie auf **Weiter**, um mit den Dialogfenstern **Clients auswählen** und **Taskbericht** fortzufahren. Eine Beschreibung dieser Fenster finden Sie im Kapitel Tasks 48.

5.1.8 Interaktiver Task

Dieser Task weicht in seiner Ausführung und Übermittlung von allen anderen hier beschriebenen Tasktypen ab.

Auf der Registerkarte **Clients** sehen Sie in der Spalte **Schutzstatus-Text** den Schutzstatus aller verbundenen ESET-Clients. Ein leeres Feld bedeutet, dass der jeweilige Client die Schutzstufe **Maximaler Schutz** hat. Bei einer niedrigeren Schutzstufe erscheint in der Spalte **Schutzstatus-Text** eine rot oder orange hervorgehobene Warnung (z. B. **ESET Personal Firewall ist deaktiviert**).

In ERA können Sie als Administrator die betreffenden Probleme direkt von der Registerkarte **Clients** aus beheben. Gehen Sie hierzu wie folgt vor:

1) Doppelklicken Sie auf der Registerkarte **Clients** auf den Eintrag eines Clients mit einer Schutzstatus-Warnung.

2) Das Dialogfenster **Eigenschaften** wird angezeigt. Klicken Sie auf die Registerkarte **Schutzstatus**.

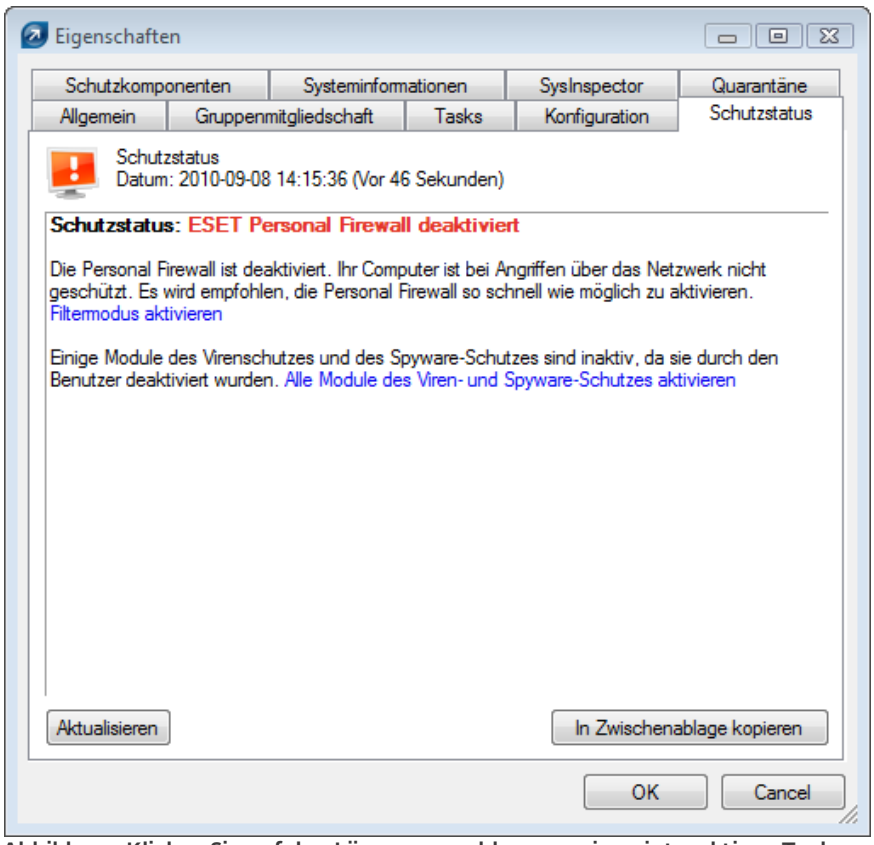

Eigenschaften
Schutzkomponenten
Systeminformationen
SysInspector
Quarantäne
Allgemein
Gruppenmitgliedschaft
Tasks
Konfiguration
Schutzstatus
Schutzstatus
Datum: 2010-09-08 14:15:36 (Vor 46 Sekunden)
Schutzstatus: ESET Personal Firewall deaktiviert
Die Personal Firewall ist deaktiviert. Ihr Computer ist bei Angriffen über das Netzwerk nicht geschützt. Es wird empfohlen, die Personal Firewall so schnell wie möglich zu aktivieren.
Filtermodus aktivieren
Einige Module des Virenschutzes und des Spyware-Schutzes sind inaktiv, da sie durch den Benutzer deaktiviert wurden. Alle Module des Viren- und Spyware-Schutzes aktivieren
Aktualisieren
In Zwischenablage kopieren
OK
Cancel

Abbildung: Klicken Sie auf den Lösungsvorschlag, um einen interaktiven Task an den Client zu senden.

3) Im Feld **Schutzstatus** sehen Sie nun ein oder mehrere Warnungen. Klicken Sie hinter einer Warnung auf den blauen Text mit dem Lösungsvorschlag.

4) Klicken Sie auf **Ja**, um die Ausführung des interaktiven Tasks zu bestätigen.

5) Wiederholen Sie die Schritte 3 und 4 für jede angezeigte Warnung. Klicken Sie dann einige Male auf **Aktualisieren**, um zu sehen, ob die Warnmeldungen verschwinden.

Sobald Sie alle Probleme behoben haben, wechselt die Schutzstatus-Meldung auf **Schutzstatus: Das System ist sicher** .

HINWEIS: Interaktive Tasks werden erst ab ESET Smart Security/ESET NOD32 Version 3 unterstützt.

5.2 Gruppen-Manager

Der Gruppen-Manager ist ein leistungsstarkes Werkzeug zur Verwaltung Ihrer Clients. Hier können Sie Clients in Gruppen zusammenfassen, um diesen unterschiedliche Einstellungen, Tasks, Einschränkungen usw. zuzuweisen. Um ihn zu öffnen, verwenden Sie einfach den Menübefehl **Extras > Gruppen-Manager** oder drücken **Strg+G**. Gruppen werden für jeden ERAS separat gespeichert und nicht repliziert.
Sie können entweder nach Bedarf eigene Gruppen analog zur Struktur Ihres Firmennetzwerks anlegen oder aber die ERAC-Clientgruppen bequem mit Ihrem Microsoft Active Directory abgleichen. Hierzu verwenden Sie die Option **Active Directory-Synchronisierung** im Hauptfenster des Gruppen-Managers.

Es gibt zwei grundlegende Arten von Clientgruppen:
- Statische Gruppen
- Parametrische Gruppen

Mit statischen und parametrischen Gruppen können Sie sich die Verwaltung von Clients in ERA an vielen Stellen erleichtern.

5.2.1 Statische Gruppen

Über statische Gruppen können Sie die Clients in Ihrem Netzwerk in benannte Gruppen und Untergruppen untergliedern. Beispielsweise könnten Sie eine Gruppe „Marketing" mit allen Clients aus der Marketingabteilung erstellen und zusätzlich Untergruppen für einzelne Teams und Unterabteilungen definieren (Innenvertrieb, Vertriebsleitung usw.).

Das Hauptfenster zur Verwaltung von statischen Gruppen gliedert sich in zwei Bereiche. Links werden die vorhandenen Gruppen in einer Hierarchie aus Gruppen und Untergruppen angezeigt. Rechts sehen Sie die Clients, die der ausgewählten Gruppe angehören. Standardmäßig werden nur die Clients in der ausgewählten Gruppe aufgeführt. Um auch die Clients aus den Untergruppen der aktuell ausgewählten Gruppe zu sehen, aktivieren Sie das Kontrollkästchen **Clients in Untergruppen anzeigen** im rechten Teil des Fensters.

Um eine neue Gruppe zu erstellen, klicken Sie auf **Erstellen** und geben einen Namen für die Gruppe ein. Die neue Gruppe wird als Untergruppe der aktuell ausgewählten Gruppe angelegt. Um eine Gruppe auf oberster Ebene zu erstellen, wählen Sie den Stammeintrag der Hierarchie aus (**Statische Gruppen**). Das Feld „Übergeordnete Gruppe" enthält den Namen der Gruppe, der die neue Gruppe untergeordnet wird (für den Stammeintrag ist dies „/"). Es empfiehlt sich, einen Namen zu wählen, aus dem der Standort der Computer ersichtlich wird (z. B. *Finanzabteilung*, *Support* usw.). Über das Beschreibungsfeld können Sie weitere Informationen zur Gruppe eingeben (z. B. *„Computer in Büro 217"*, *„Arbeitsplatzrechner in der Zentrale"* usw.). Neu erstellte und konfigurierte Gruppen können Sie später selbstverständlich noch bearbeiten.

HINWEIS: Wenn Sie einen Task für eine bestimmte Gruppe definieren, wird er auch auf allen Clients in ihren Untergruppen ausgeführt.

Sie können auch leere Gruppen erstellen, die Sie erst später verwenden möchten.

Klicken Sie auf **OK**, um die Gruppe anzulegen. Ihr Name und ihre Beschreibung erscheinen im linken Teil des Fensters, und die Schaltfläche **Hinzufügen/Entfernen** ist nun verfügbar. Klicken Sie darauf, um der Gruppe die gewünschten Clients hinzuzufügen (entweder per Doppelklick oder per Drag&Drop aus der linken in die rechte Liste). Um schnell Clients mit einem bestimmten Namen zu finden, geben Sie den Namen ganz oder teilweise im Feld **Schnellsuche** ein. Daraufhin werden alle Clients angezeigt, deren Name den eingegebenen Text enthält. Um alle Clients auszuwählen, klicken Sie auf **Alle auswählen**. Um zu prüfen, ob in der Zwischenzeit weitere Clients eine Verbindung zum Server aufgebaut haben, können Sie die Anzeige über die Schaltfläche **Aktualisieren** neu aufbauen.

Wenn die manuelle Auswahl der Clients zu aufwendig wird, können Sie über die Schaltfläche **Hinzufügen (erweitert)** auf weitere Optionen zugreifen.

Aktivieren Sie die Option **Im Clientbereich geladene Clients hinzufügen**, um alle auf der Registerkarte „Clients" angezeigten Clients hinzuzufügen. Diese Option können Sie mit dem Kontrollkästchen **Nur ausgewählte** auch noch weiter einschränken. Um Clients hinzuzufügen, die bereits einem anderen Server oder einer anderen Gruppe angehören, wählen Sie sie aus der entsprechenden Liste aus (Server links, Gruppen rechts) und klicken auf **Hinzufügen**.

Um zur Verwaltung der statischen Gruppen im Hauptfenster des Gruppen-Managers zurückzukehren, klicken Sie im Dialogfenster **Hinzufügen/Entfernen** auf **OK**. Die neue Gruppe wird nun mit den ausgewählten Clients angezeigt.

Klicken Sie auf **Hinzufügen/Entfernen**, um Clients zu einer Gruppe hinzuzufügen oder daraus zu entfernen, oder auf **Löschen**, um eine Gruppe komplett zu löschen. Um die Client- und Gruppenliste zu kopieren, klicken Sie auf **In Zwischenablage kopieren**. Zum Aktualisieren der Clientliste klicken Sie auf **Aktualisieren**.

Sie können die Clients der aktuell ausgewählten Gruppe auch als *.xml*-Datei importieren oder exportieren (Schaltfläche **Importieren/Exportieren**).

5.2.2 Parametrische Gruppen

Neben statischen Gruppen sind auch parametrische Gruppen ein sehr leistungsstarkes Werkzeug. Bei einer parametrischen Gruppe werden die Clients dynamisch der Gruppe zugeordnet, je nachdem, ob sie die Bedingungen der Gruppe erfüllen. Diese parametrischen Gruppen können Sie dann an einer Reihe von Stellen anstelle einer statischen Gruppe verwenden, etwa in Filtern, Policies, Berichten und Notifikationen.

Das Hauptfenster zur Einrichtung parametrischer Gruppen gliedert sich in vier Bereiche. Die Liste **Parametrische Gruppen** zeigt die von Ihnen erstellten Gruppen samt Untergruppen. Wenn Sie hier eine bestimmte Gruppe auswählen, werden die Clients aus dieser Gruppe im Bereich **Ausgewählte Gruppe** angezeigt.
HINWEIS: Wenn Sie eine übergeordnete Gruppe auswählen, umfasst die Liste auch den Inhalt der Untergruppen.

Die eingestellten Parameter für die ausgewählte Gruppe werden im Bereich **Parameter** angezeigt. Über die Schaltfläche **Bearbeiten** können Sie jederzeit Parameter bearbeiten oder hinzufügen.

Im Bereich **Status der Synchronisierung** wird über eine Fortschrittsleiste der aktuelle Stand der Synchronisierung angezeigt.

Um eine neue Gruppe zu erstellen, klicken Sie einfach auf **Erstellen**. Die neue Gruppe wird als Untergruppe der aktuell ausgewählten Gruppe angelegt. Um eine Gruppe auf oberster Ebene zu erstellen, wählen Sie den Stammeintrag der Hierarchie aus (**Parametrische Gruppen**). Das Feld „Übergeordnete Gruppe" enthält den Namen der Gruppe, der die neue Gruppe untergeordnet wird (für den Stammeintrag ist dies „/"). Geben Sie den **Namen** und eine kurze **Beschreibung** für die neue Gruppe ein. Richten Sie dann unter **Client-Filter-Parameter** die gewünschten Kriterien für die Gruppe ein, indem Sie auf **Bearbeiten** klicken und die passenden Optionen auswählen. Wenn Sie das Kontrollkästchen **Permanent** aktivieren, werden Clients, die die Bedingungen erfüllen, automatisch in die Gruppe aufgenommen und anschließend nie wieder daraus entfernt. Der Inhalt einer Gruppe, für die die Einstellung „Permanent" aktiviert ist, kann auf der Stammebene manuell zurückgesetzt werden.

HINWEIS: Dieser Parameter kann nur beim Erstellen einer neuen Gruppe verändert werden.

Um eine vorhandene Gruppe zu bearbeiten, wählen Sie sie in der Liste **Parametrische Gruppen** aus und klicken dann im unteren Teil des Fensters auf **Bearbeiten**. Zum Löschen einer Gruppe wählen Sie sie aus und klicken auf **Löschen**. Sie können die Anzeige der Gruppenliste von Hand aktualisieren, indem Sie auf **Aktualisieren** klicken. Um eine Gruppe aus einer Datei zu importieren, wählen Sie zunächst in der Liste **Parametrische Gruppen** die Gruppe aus, der die importierte Gruppe untergeordnet werden soll. Klicken Sie dann auf **Importieren**. Bestätigen Sie Ihre Auswahl durch Klicken auf **Ja**. Wählen Sie die gewünschte Datei für den Import aus und klicken Sie auf **Öffnen**. Die Gruppe wird mitsamt allen Untergruppen importiert und an der ausgewählten Stelle in die Hierarchie eingefügt. Um eine Gruppe mit allen Untergruppen zu exportieren, wählen Sie sie in der Liste **Parametrische Gruppen** aus, klicken auf den Pfeil neben der Schaltfläche **Importieren** und wählen **Exportieren**. Klicken Sie zur Bestätigung auf **Ja**, wählen Sie einen Namen und einen Speicherort für die Exportdatei aus und klicken Sie auf **Speichern**.

HINWEIS: Vorhandene Gruppen in der Liste **Parametrische Gruppen** können Sie per Drag&Drop verschieben.

5.2.3 Active Directory-Synchronisierung

Bei der Active Directory-Synchronisierung werden ausgehend von der im Active Directory (AD) definierten Struktur automatisch passende Gruppen mit den entsprechenden Clients erstellt. Als Administrator können Sie so sehr komfortabel Clients in Gruppen zusammenfassen. Voraussetzung hierfür ist, dass die Clients im AD unter ihrem Namen als Objekte des Typs *Computer* vorhanden sind und AD-Gruppen angehören.

Der Ablauf der Synchronisierung wird durch zwei grundlegende Optionen gesteuert:

Über die Option **Gruppen synchronisieren** legen Sie fest, welche AD-Gruppen synchronisiert werden sollen. Die Einstellung **Alle Gruppen** bewirkt, dass die komplette AD-Hierarchie synchronisiert wird, unabhängig davon, ob die AD-Gruppen tatsächlich ERA-Clients enthalten. Bei den beiden anderen Einstellungen (**Nur Gruppen mit Clients des ERA Servers** und **Nur Gruppen mit primären Clients des ERA-Servers**) wird die Synchronisierung hingegen eingeschränkt, d. h. es werden nur Gruppen synchronisiert, die vorhandene ERA-Clients enthalten.

Mit der Option **Synchronisierungsart** legen Sie fest, ob die zu synchronisierenden AD-Gruppen zu den vorhandenen AD-Gruppen hinzugefügt werden (**AD-Gruppen importieren**) oder diese vollständig ersetzen sollen (**AD-Gruppen synchronisieren**).

Über die Option **Synchronisieren** können Sie wahlweise ein Intervall für die AD-Synchronisierung festlegen.

Weitere Einstellungen für die Active Directory-Synchronisierung können Sie über den Konfigurationseditor einrichten (**ESET Remote Administrator** > **ERA Server** > **Einstellungen** > **Gruppen** > **Optionen für Active Directory-Synchronisierung**). Standardmäßig werden nur **Computer-Sicherheitsgruppen und Computer-Organisationseinheiten** synchronisiert. Sie können jedoch auch andere Active Directory-Objekte einbeziehen, indem Sie die gewünschte Option aktivieren.

HINWEIS: Für die Active Directory-Synchronisierung muss ERAS nicht auf dem Domänencontroller installiert sein. Es reicht aus, wenn der Rechner, auf dem ERAS installiert ist, auf den Domänencontroller zugreifen kann. Um die Authentifizierung für Ihren Domänencontroller zu konfigurieren, verwenden Sie die Option **Extras** > **Serveroptionen** > **Erweitert** > **Erweiterte Einstellungen bearbeiten...** > **ESET Remote Administrator** > **ERA Server** > **Einstellungen** > **Active Directory**. Der Servername wird im Format *LDAP://Servername* oder *GC://Servername* angegeben. Fehlt diese Angabe, wird der globale Katalog (GC) verwendet.

5.3 Policies

Policies ähneln in vielerlei Hinsicht Konfigurations-Tasks. Allerdings handelt es sich hierbei nicht um einmalige Tasks, die an einen oder mehrere Arbeitsplatzrechner übermittelt werden. Sie dienen vielmehr dazu, bestimmte Konfigurationseinstellungen für ESET Security-Produkte dauerhaft aufrechtzuerhalten. Bei einer Policy handelt es sich also um eine Konfiguration, deren Durchsetzung auf dem Client erzwungen wird.

5.3.1 Grundsätze und Funktionsweise

Zum Öffnen des Policy-Managers wählen Sie den Menüpunkt **Extras** > **Policy-Manager**. Die Policyhierarchie im linken Teil des Fensters zeigt die Policies auf den einzelnen Servern. Der rechte Teil des Fensters gliedert sich in vier Bereiche: **Policyeinstellungen**, **Policykonfiguration**, **Policyaktionen** sowie **Globale Policyeinstellungen**. Mit den Optionen in diesen Bereichen können Sie als Administrator Policies verwalten und konfigurieren.

Der Policy-Manager dient primär zum Erstellen, Bearbeiten und Entfernen von Policies. Die Clients erhalten die Policies von ERAS. ERAS kann mehrere Policies verwenden, die ihre Einstellungen voneinander oder von Policies von einem übergeordneten Server erben können.

Dieses System der Übernahme von Policies von einem übergeordneten Server wird als *Vererbung* bezeichnet. Policies, die als Ergebnis einer solchen Vererbung erstellt werden, heißen *zusammengeführte Policies*. Die Vererbung basiert auf einer hierarchischen Struktur: Untergeordnete Policies erben die Einstellungen der übergeordneten Policies.

5.3.2 Erstellen von Policies

Nach der Installation ist standardmäßig nur eine einzige Policy namens „Server-Policy" implementiert. Diesen Namen können Sie unter **Policyeinstellungen** im Feld **Name der Policy** ändern. Die Policy selbst können Sie im ESET Configuration Editor konfigurieren. Klicken Sie dazu auf **Bearbeiten** und definieren Sie die Parameter für das ausgewählte ESET Security-Produkt (Client). Die Parameter sind in einer umfassenden Baumstruktur gegliedert. Jedes Konfigurationselement wird im Editor mit einem Symbol angezeigt. Blaue Symbole stehen dabei für aktive Parameter, die auf den Clients übernommen werden. Alle inaktiven Parameter (graue Symbole) bleiben auf den Zielcomputern hingegen unverändert. Dieses Prinzip gilt auch für geerbte und zusammengeführte Policies; untergeordnete Policies übernehmen aus der übergeordneten Policy jeweils nur die aktiven Parameter.

Sie können in ERA Server mehrere Policies definieren (Schaltfläche **Neue untergeordnete Policy hinzufügen**). Die wesentlichen Optionen für eine neue Policy sind ihr Name, die Verknüpfung **Übergeordnete Policy** sowie die Konfiguration. Letztere kann entweder leer sein oder aber aus einer vorhandenen Policy oder einer *.xml*-Konfigurationsdatei kopiert werden. Policies können jeweils nur auf dem Server erstellt werden, mit dem Sie gerade in ERAC verbunden sind. Um eine Policy auf einem untergeordneten Server zu erstellen, müssen Sie direkt eine Verbindung zu diesem Server aufbauen.

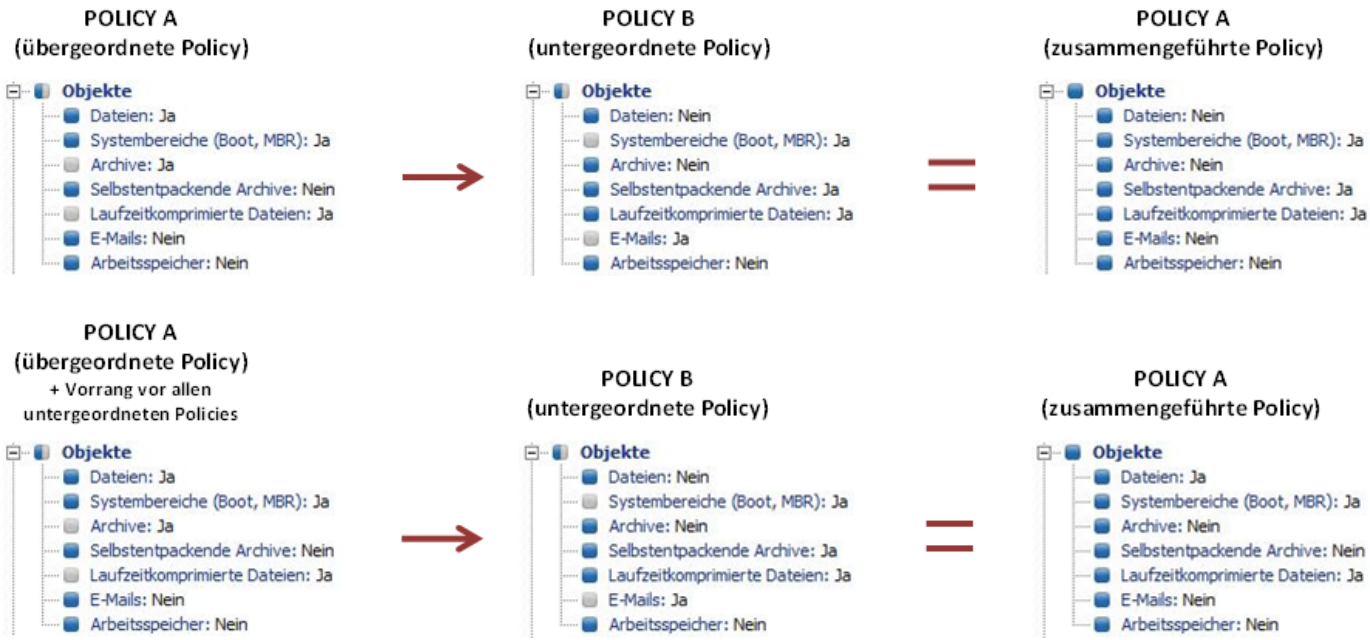
Jede Policy hat zwei grundlegende Attribute: **Vorrang vor allen untergeordneten Policies** sowie **Kann auf untergeordnete Server repliziert werden**. Diese Attribute legen fest, wie aktive Konfigurationsparameter in untergeordneten Policies übernommen werden.

Vorrang vor allen untergeordneten Policies - Erzwingt die Durchsetzung aller aktiven Parameter bei der Vererbung. Falls in der untergeordneten Policy andere Einstellungen für einen aktiven Parameter festgelegt sind, werden diese in

der zusammengeführten Policy mit den betreffenden Einstellungen der vererbten übergeordneten Policy überschrieben. Dies gilt auch dann, wenn die Option **Vorrang vor allen ...** in der untergeordneten Policy selbst wiederum aktiviert ist. Parameter, die in der übergeordneten Policy inaktiv sind, richten sich nach den Einstellungen in der untergeordneten Policy. Wenn das Attribut **Vorrang vor allen untergeordneten Policies** nicht aktiviert ist, haben die Einstellungen aus der untergeordneten Policy beim Zusammenführen hingegen Vorrang vor denen der übergeordneten Policy. Falls der solchermaßen zusammengeführten Policy weitere Policies untergeordnet sind, wird sie dort nach demselben Muster übernommen.

Kann auf untergeordnete Server repliziert werden - Aktiviert die Replikation auf untergeordnete Policies, d. h. die Policy kann als Standardpolicy für untergeordnete Server dienen und Clients zugewiesen werden, die mit untergeordneten Servern verbunden sind.

Sie können Policies auch über *.xml*-Dateien importieren und exportieren oder aus Gruppen importieren. Nähere Informationen finden Sie im Kapitel Importieren/Exportieren von Policies 58.



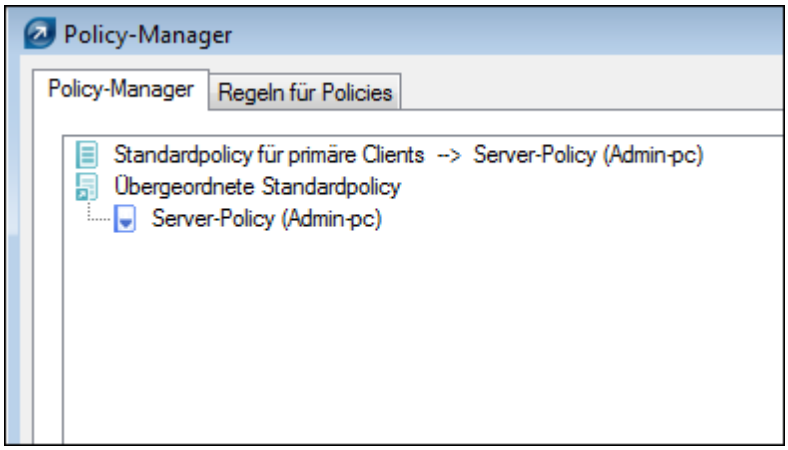
5.3.3 Virtuelle Policies

Neben den von Ihnen erstellten und den von anderen Servern replizierten Policies (siehe Kapitel Replikation (Registerkarte) 84) enthält die Policyhierarchie auch eine „Übergeordnete Standardpolicy“ sowie eine „Standardpolicy für primäre Clients“. Hierbei handelt es sich um so genannte „virtuelle Policies“.

Die übergeordnete Standardpolicy ist die Policy, die auf einem übergeordneten Server in den globalen Policyeinstellungen als **Standardpolicy für untergeordnete Server** ausgewählt wurde. Wenn der Server nicht repliziert wird, ist diese Policy leer (nähere Informationen hierzu später).

Die „Standardpolicy für primäre Clients“ wird auf dem jeweiligen Server (also nicht auf einem übergeordneten Server) in den globalen Policyeinstellungen definiert und erscheint unter diesem Namen in der Policyhierarchie. Sie wird auf neu verbundenen Clients (primären Clients) des betreffenden ERAS automatisch durchgesetzt, sofern diesen Clients nicht bereits mithilfe von Policyregeln eine andere Policy zugewiesen wurde (nähere Informationen siehe Kapitel Zuweisen von Policies zu Clients 58). Virtuelle Policies sind also Verknüpfungen zu anderen Policies, die sich auf demselben Server befinden.

5.3.4 Rolle und Zweck von Policies in der Policyhierarchie



Neben jeder Policy in der Policyhierarchie steht links ein Symbol. Diese Symbole haben die folgende Bedeutung:

1. Policies mit blauen Symbolen sind auf dem jeweiligen Server vorhanden. Das blaue Symbol hat drei Untertypen:

Symbole mit weißer Füllung: Die Policy wurde auf dem jeweiligen Server erstellt. Sie kann nicht auf untergeordnete Server repliziert werden, d. h. sie ist keinen Clients von untergeordneten Servern zugewiesen und dient auch nicht als übergeordnete Policy für die untergeordneten Server. Solche Policies können also nur Clients zugewiesen werden, die direkt mit dem jeweiligen Server verbunden sind. Außerdem können sie als übergeordnete Policies für andere Policies auf demselben Server dienen.

Symbole mit blauer Füllung: Die Policy wurde ebenfalls auf dem Server erstellt, aber mit aktivierter Option **Vorrang vor allen untergeordneten Policies** (nähere Informationen finden Sie im Kapitel Erstellen von Policies 55).

Symbole mit Pfeilen nach unten: Für diese Policies ist die Option **Kann auf untergeordnete Server repliziert werden** aktiviert, d. h. sie werden repliziert. Sie können solche Policies sowohl auf dem aktuellen Server als auch auf seinen untergeordneten Servern anwenden.

2. Policies mit grauen Symbolen stammen von anderen Servern.

Symbole mit Pfeilen nach oben: Diese Policies wurden von einem untergeordneten Server repliziert. Sie können lediglich angezeigt und (über die Schaltfläche **Policy-Zweig löschen**) gelöscht werden. Hiermit wird die eigentliche Policy nicht gelöscht, sondern nur aus der Policyhierarchie entfernt. Nach einer erneuten Replikation wird sie daher unter Umständen wieder angezeigt. Wenn keine Policies von untergeordneten Servern angezeigt werden sollen, aktivieren Sie die Option **Policies anderer Server ausblenden, wenn nicht in Policyhierarchie verwendet**.

Symbole mit Pfeilen nach unten: Diese Policies wurden von einem übergeordneten Server repliziert. Sie können anderen Policies übergeordnet, Clients zugewiesen (**Clients hinzufügen**) oder entfernt werden (**Policy löschen**). Bitte beachten Sie, dass die eigentliche Policy auch hier nicht gelöscht wird und daher nach der nächsten Replikation vom übergeordneten Server wieder erscheint (sofern nicht in der Zwischenzeit die Option **Kann auf untergeordnete Server repliziert werden** auf dem übergeordneten Server deaktiviert wurde).

HINWEIS: Um die Position einer Policy in der Hierarchie zu verändern, können Sie entweder die Einstellung „Übergeordnete Policy“ ändern oder die Policy per Drag&Drop mit der Maus verschieben.

Um vorhandene Policyregeln über eine *.xml*-Datei zu importieren/exportieren, klicken Sie auf **Importieren/Exportieren**. Wenn beim Import ein Namenskonflikt auftritt (d. h. die zu importierende Policy hat denselben Namen wie eine bereits vorhandene Policy), wird dieser gelöst, indem an den Namen der importierten Policy eine zufällig gewählte Zeichenfolge angehängt wird.

5.3.5 Anzeigen von Policies

Policies aus der Policyhierarchie können Sie direkt im Configuration Editor anzeigen, indem Sie auf **Anzeigen** oder **Zusammengeführt anzeigen** klicken.

Zusammengeführt anzeigen - Zeigt die zusammengeführte Policy an, die als Ergebnis der Vererbung (Übernahme von Einstellungen) von übergeordneten Policies entsteht. Diese Option wird standardmäßig angezeigt, weil es sich bei der aktuellen Policy bereits um eine zusammengeführte Policy handelt.

Anzeigen - Zeigt die ursprüngliche Policy vor ihrer Zusammenführung mit der übergeordneten Policy an.

Auf untergeordneten Servern stehen für Policies, die von übergeordneten Servern geerbt wurden, die folgenden Optionen zur Verfügung:

Zusammengeführt anzeigen - siehe oben

Überschreibenden Teil anzeigen - Diese Schaltfläche ist für Policies relevant, bei denen die Option „Vorrang vor allen untergeordneten Policies" aktiv ist. Sie zeigt gezielt den überschreibenden Teil der Policy an, d. h. den Teil, der abweichende Einstellungen in untergeordneten Policies außer Kraft setzt.

Nicht überschreibenden Teil anzeigen - Funktioniert umgekehrt wie der Befehl „Überschreibenden Teil anzeigen", d. h. es werden nur aktive Einträge angezeigt, für die die Option „Vorrang vor allen..." nicht aktiviert ist.

5.3.6 Importieren/Exportieren von Policies

Über den Policy-Manager können Sie Policies sowie Policyregeln importieren und exportieren. Um vorhandene Policies über eine *.xml*-Datei zu importieren/exportieren, klicken Sie auf **Policies importieren/Policies exportieren**. Darüber hinaus ist mit der Schaltfläche **Aus Gruppen importieren** ein Import von Policies aus Gruppen möglich. Zum Importieren/Exportieren von Policyregeln klicken Sie auf **Importieren/Exportieren**. Außerdem können Sie Policyregeln auch über den **Assistenten für Policyregeln** erstellen.

Wenn beim Import ein Namenskonflikt auftritt (d. h. die zu importierende Policy hat denselben Namen wie eine bereits vorhandene Policy), wird dieser gelöst, indem an den Namen der importierten Policy eine zufällig gewählte Zeichenfolge angehängt wird. Falls dies im Einzelfall nicht funktioniert (wenn z. B. der neue Name zu lang ist), wird der Importvorgang mit der Warnung *Nicht aufgelöster Policyregel-Namenskonflikt* abgeschlossen. Um den Konflikt in solch einem Fall aufzulösen, müssen Sie die betreffenden Policies bzw. Policyregeln löschen oder umbenennen.

5.3.7 Zuweisen von Policies zu Clients

Für die Zuweisung von Policies zu Clients gibt es zwei wesentliche Regeln:

1. Lokalen (primären) Clients können Sie beliebige lokale Policies oder Policies, die von übergeordneten Servern repliziert wurden, zuweisen.

2. Einem Client, der von einem untergeordneten Server repliziert wurde, können Sie beliebige lokale Policies zuweisen, für die die Einstellung **Kann auf untergeordnete Server repliziert werden** aktiviert ist, sowie alle Policies, die von übergeordneten Servern repliziert wurden. Sie können dem Client jedoch keine Policies von seinem eigenen primären Server zuweisen. Hierzu müssen Sie in ERAC eine Verbindung zu diesem Server aufbauen.

Beachten Sie die folgenden wichtigen Hinweise: Prinzipiell wird jedem Client eine Policy zugewiesen. Einen „Client ohne Policy" gibt es nicht. Außerdem ist es nicht möglich, eine Policy von einem Client zu entfernen. Sie können sie lediglich durch eine andere Policy ersetzen. Wenn ein bestimmter Client überhaupt keine Konfiguration über eine Policy erhalten soll, erstellen Sie eine leere Policy und weisen dem Client diese zu.

5.3.7.1 Standardpolicy für primäre Clients

Eine Methode zum Zuweisen von Policies ist die automatische Anwendung der Standardpolicy für primäre Clients. Hierbei handelt es sich um eine virtuelle Policy, die in den globalen Policyeinstellungen konfiguriert werden kann. Sie wird den primären Clients zugewiesen, d. h. den Clients mit einer direkten Verbindung zum jeweiligen ERAS. Nähere Informationen finden Sie im Kapitel Virtuelle Policies 56.

5.3.7.2 Manuelle Zuweisung

Um Policies manuell zuzuweisen, gibt es zwei Möglichkeiten: Entweder klicken Sie mit der rechten Maustaste auf einen Eintrag auf der Registerkarte **Clients** und wählen dann im Kontextmenü den Befehl **Policy hinzufügen**, oder Sie klicken im Policy-Manager auf **Clients hinzufügen** > **Hinzufügen/Entfernen**.

Durch Klicken auf **Clients hinzufügen** im Policy-Manager wird das Dialogfenster **Hinzufügen/Entfernen** geöffnet. Im linken Teil des Fensters sind die Clients im Format Server/Client aufgeführt. Wenn die Option **Kann auf untergeordnete Server repliziert werden** aktiv ist, umfasst die Liste auch Clients, die von untergeordneten Servern repliziert wurden. Wählen Sie die Clients, denen die Policy zugewiesen werden soll, entweder per Drag&Drop aus oder verschieben Sie sie durch Klicken auf **>>** in die Liste **Ausgewählte Objekte**. Neu ausgewählte Clients werden mit einem gelben Sternchen angezeigt. Sie haben jetzt noch die Möglichkeit, sie wieder aus der Liste **Ausgewählte Objekte** zu entfernen; klicken Sie dazu auf **<<** (einzeln entfernen) oder **C** (alle entfernen). Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.

HINWEIS: Nachdem Sie die Zuweisung einmal bestätigt haben, können Sie die Clients im Dialogfenster **Hinzufügen/ Entfernen** nicht mehr aus der Liste **Ausgewählte Objekte** entfernen. Sie können lediglich die Policy durch eine andere ersetzen.

Zum Hinzufügen von Clients können Sie auch die Funktion **Hinzufügen (erweitert)** verwenden. Auf diese Weise können Sie alle Clients auf einmal, nur die ausgewählten Clients oder alle Clients eines bestimmten Servers bzw. einer Gruppe hinzufügen.

5.3.7.3 Policyregeln

Mit dem Werkzeug **Regeln für Policies** können Sie als Administrator die Zuweisung von Policies zu Clients umfassend und komfortabel automatisieren. Regeln werden ausgeführt, sobald der Client eine Verbindung zum Server aufbaut. Sie haben Vorrang vor der **Standardpolicy für primäre Clients** und vor manuell zugewiesenen Policies. Die **Standardpolicy für primäre Clients** wird nur verwendet, wenn der Client durch keine der aktuellen Regeln abgedeckt wird. Wenn einem Client manuell eine Policy zugewiesen wurde, die in Konflikt mit den Policyregeln steht, hat die von den Policyregeln erzwungene Konfiguration Vorrang.

Zum Erstellen und Verwalten von Policyregeln gibt es eine eigene Registerkarte im Policy-Manager. Die Erstellung und Anwendung der Regeln läuft in vielerlei Hinsicht ähnlich ab wie das Erstellen und Verwalten von Regeln in E-Mail-Programmen. Jede Regel kann ein oder mehrere Kriterien enthalten und in der Regelliste nach oben oder unten verschoben werden. Je weiter oben die Regel in der Liste steht, desto höher ist ihre Priorität.

Um eine neue Regel zu erstellen, klicken Sie auf **Neu**. Tragen Sie dann die gewünschten Werte in die Felder **Name**, **Beschreibung**, **Client-Filter-Parameter** sowie **Policy** ein (letzteres ist die Policy, die den Clients zugewiesen wird, die die angegebenen Kriterien erfüllen).

Um die Filterkriterien zu konfigurieren, klicken Sie auf **Bearbeiten**.

Die folgenden Kriterien stehen zur Verfügung:

(NICHT) VON Primärer Server - Erfüllt, wenn sich der Client (nicht) auf dem primären Server befindet.
IST (NICHT) Neuer Client - Erfüllt, wenn es sich (nicht) um einen neuen Client handelt.
HAT (NICHT) Markierung „Neu“ - Erfüllt, wenn für den Client die Markierung „Neu“ (nicht) gesetzt ist.
Primärer Server (NICHT) IN (festlegen) - Erfüllt, wenn der Name des primären Servers die angegebene Zeichenfolge (nicht) enthält.
ERA-Gruppen IN (festlegen) - Erfüllt, wenn der Client der angegebenen Gruppe angehört.
ERA-Gruppen NICHT IN (festlegen) - Erfüllt, wenn der Client der angegebenen Gruppe nicht angehört.
Domäne/Arbeitsgruppe (NICHT) IN (festlegen) - Erfüllt, wenn der Client der angegebenen Domäne (nicht) angehört.
Maske für Computernamen IN (festlegen) - Erfüllt, wenn der Client den angegebenen Computernamen hat.
HAT IP-Maske (festlegen) - Erfüllt, wenn die IP-Adresse des Clients in dem durch IP-Adresse und Maske angegebenen Netzwerk liegt.
HAT IP-Bereich (festlegen) - Erfüllt, wenn die IP-Adresse des Clients im angegebenen Bereich liegt.
HAT (NICHT) Festgelegte Policy (festlegen) - Erfüllt, wenn der Client die angegebene Policy (nicht) verwendet.
Produktname (NICHT) IN - Erfüllt, wenn der angegebene Produktname (nicht) vorliegt.

Produktversion IST (NICHT) - Erfüllt, wenn die angegebene Produktversion (nicht) vorliegt.
Maske für benutzerdefinierte Clientinfos (NICHT) IN - Erfüllt, wenn die benutzerdefinierten Clientinfos die angegebene Zeichenfolge (nicht) enthalten.
HAT (NICHT) Schutzstatus (festlegen) - Erfüllt, wenn auf dem Client der angegebene Schutzstatus (nicht) vorliegt.
Signaturdatenbank-Version IST (NICHT) - Erfüllt, wenn die angegebene Version der Signaturdatenbank (nicht) vorliegt.
Letzte Verbindung IST (NICHT) länger her als (festlegen) - Erfüllt, wenn die letzte Verbindung (nicht) länger her ist als die angegebene Zeitspanne.
IST (NICHT) Im Zustand „Warten auf Neustart" - Erfüllt, wenn der Client (nicht) auf einen Neustart wartet.

Policyregeln können über eine *.xml*-Datei importiert/exportiert und über den **Assistenten für Policyregeln** auch automatisch erstellt werden. Mit diesem Assistenten können Sie auf der Grundlage der vorhandenen Gruppenstruktur eine passende Policystruktur erstellen und die neuen Policies über entsprechende Regeln den Gruppen zuweisen. Nähere Informationen zum Importieren/Exportieren von Policyregeln finden Sie im Kapitel Importieren/Exportieren von Policies 58.

Um eine Policyregel zu entfernen, klicken Sie im **Policy-Manager** auf **Löschen**. Um alle Regeln sofort anzuwenden, klicken Sie auf **Policyregeln jetzt anwenden**.

5.3.8 Löschen von Policies

Genau wie das Erstellen von Policies ist auch das Löschen von Policies nur auf dem Server möglich, mit dem Sie gerade verbunden sind. Um eine Policy von einem anderen Server zu löschen, müssen Sie zunächst in ERAC eine direkte Verbindung zu diesem Server aufbauen.

HINWEIS: Policies können mit anderen Servern oder Policies verknüpft sein (als übergeordnete Policy, als Standardpolicy für untergeordnete Server, als Standardpolicy für primäre Clients usw.). In bestimmten Fällen können Policies daher nicht einfach gelöscht werden, sondern müssen ersetzt werden. Um die Optionen zum Löschen und Ersetzen anzuzeigen, klicken Sie auf **Policy löschen**. Welche der nachfolgenden Optionen im konkreten Fall zur Verfügung stehen, richtet sich nach der Stellung der betreffenden Policy in der Policyhierarchie.

Neue Policy für primäre Clients mit der zu löschenden Policy - Hiermit können Sie für primäre Clients eine neue Policy als Ersatz für die zu löschende Policy festlegen. Primäre Clients können entweder die **Standardpolicy für primäre Clients** oder andere Policies vom gleichen Server übernehmen (entweder über **Clients hinzufügen** manuell zugewiesen oder über **Policyregeln** durchgesetzt). Als Ersatz können Sie eine beliebige Policy vom jeweiligen Server oder eine replizierte Policy verwenden.

Neue übergeordnete Policy für Policies unter der zu löschenden Policy (falls vorhanden) - Wenn der zu löschenden Policy andere Policies untergeordnet waren, müssen Sie ebenfalls einen Ersatz festlegen. Als Ersatz können Sie eine andere Policy vom betreffenden Server oder eine von einem übergeordneten Server replizierte Policy verwenden. Sie können auch die Option „Nicht verfügbar" wählen, um den untergeordneten Policies keine Ersatzpolicy zuzuweisen. Es empfiehlt sich jedoch dringend, sogar dann eine Ersatzpolicy zuzuweisen, wenn der zu löschenden Policy keine anderen Policies untergeordnet sind. Anderenfalls kommt es zu Konflikten, wenn parallel zum Löschvorgang ein anderer Benutzer der zu löschenden Policy eine andere Policy unterordnet.

Neue Policy für replizierte Clients mit der zu löschenden/ändernden Policy - Hiermit können Sie für Clients, die von untergeordneten Servern repliziert wurden, eine neue Policy als Ersatz für die zu löschende Policy festlegen. Als Ersatz können Sie eine beliebige Policy vom jeweiligen Server oder eine replizierte Policy verwenden.

Neue Standardpolicy für untergeordnete Server - Wenn die zu löschende Policy als virtuelle Policy dient (siehe Bereich **Globale Policyeinstellungen**), muss sie durch eine andere Policy ersetzt werden (nähere Informationen siehe Kapitel Virtuelle Policies 56). Als Ersatz können Sie eine beliebige Policy vom jeweiligen Server verwenden oder die Option „Nicht verfügbar" wählen.

Neue Standardpolicy für primäre Clients - Wenn die zu löschende Policy als virtuelle Policy dient (siehe Bereich **Globale Policyeinstellungen**), muss sie durch eine andere Policy ersetzt werden (nähere Informationen siehe Kapitel Virtuelle Policies 56). Als Ersatz können Sie eine andere Policy vom gleichen Server verwenden.

Dasselbe Dialogfenster erscheint auch, wenn Sie die Option **Kann auf untergeordnete Server repliziert werden** für eine Policy deaktivieren und auf **OK** oder **Übernehmen** klicken oder wenn Sie eine andere Policy in der Hierarchie auswählen. In diesem Fall werden die Felder **Neue Policy für replizierte Clients mit der zu löschenden/ändernden Policy** bzw. **Neue Standardpolicy für untergeordnete Server** aktiviert.

5.3.9 Erweiterte Einstellungen

Zwei weitere Einstellungen für die Zuweisung von Policies finden Sie nicht im Policy-Manager, sondern unter **Extras** > **Serveroptionen** > **Erweitert** > **Erweiterte Einstellungen bearbeiten** > **ESET Remote Administrator** > **ERA Server** > **Einstellungen > Policies**.

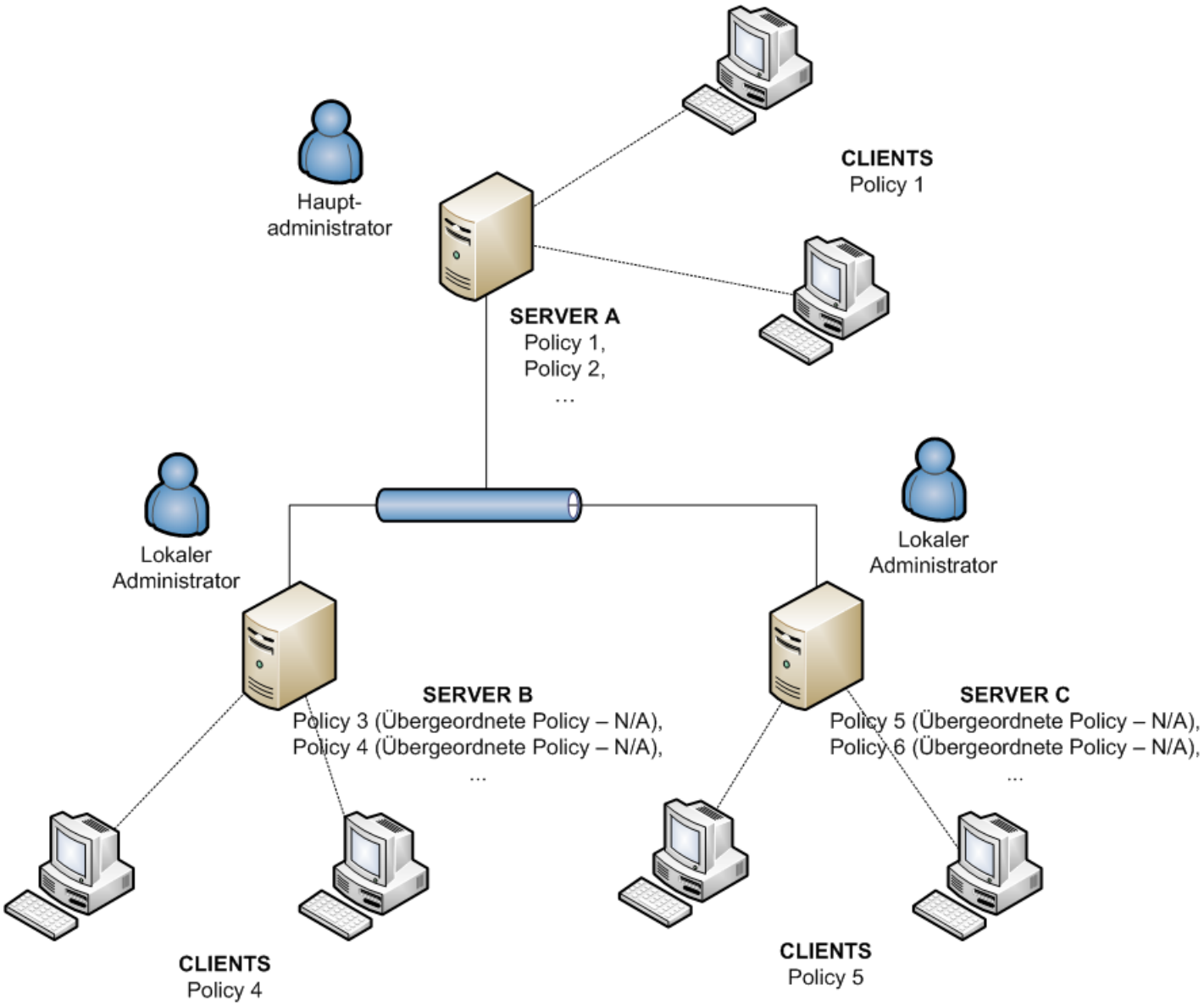
Intervall für die Durchsetzung von Policies (Minuten):
Diese Einstellung legt fest, in welchem Zeitintervall Policies übernommen werden. Die Standardeinstellung wird empfohlen.

Policynutzung deaktivieren:
Wenn Sie diese Option aktivieren, wird die Durchsetzung von Policies für einen gesamten Server deaktiviert. Sie sollten diese Option nur verwenden, wenn ein Problem mit einer bestimmten Policy vorlegt. Wenn eine Policy nur auf bestimmten Clients nicht durchgesetzt werden soll, sollten Sie diesen Clients stattdessen besser eine leere Policy zuweisen.

5.3.10 Szenarien für die Durchsetzung von Policies

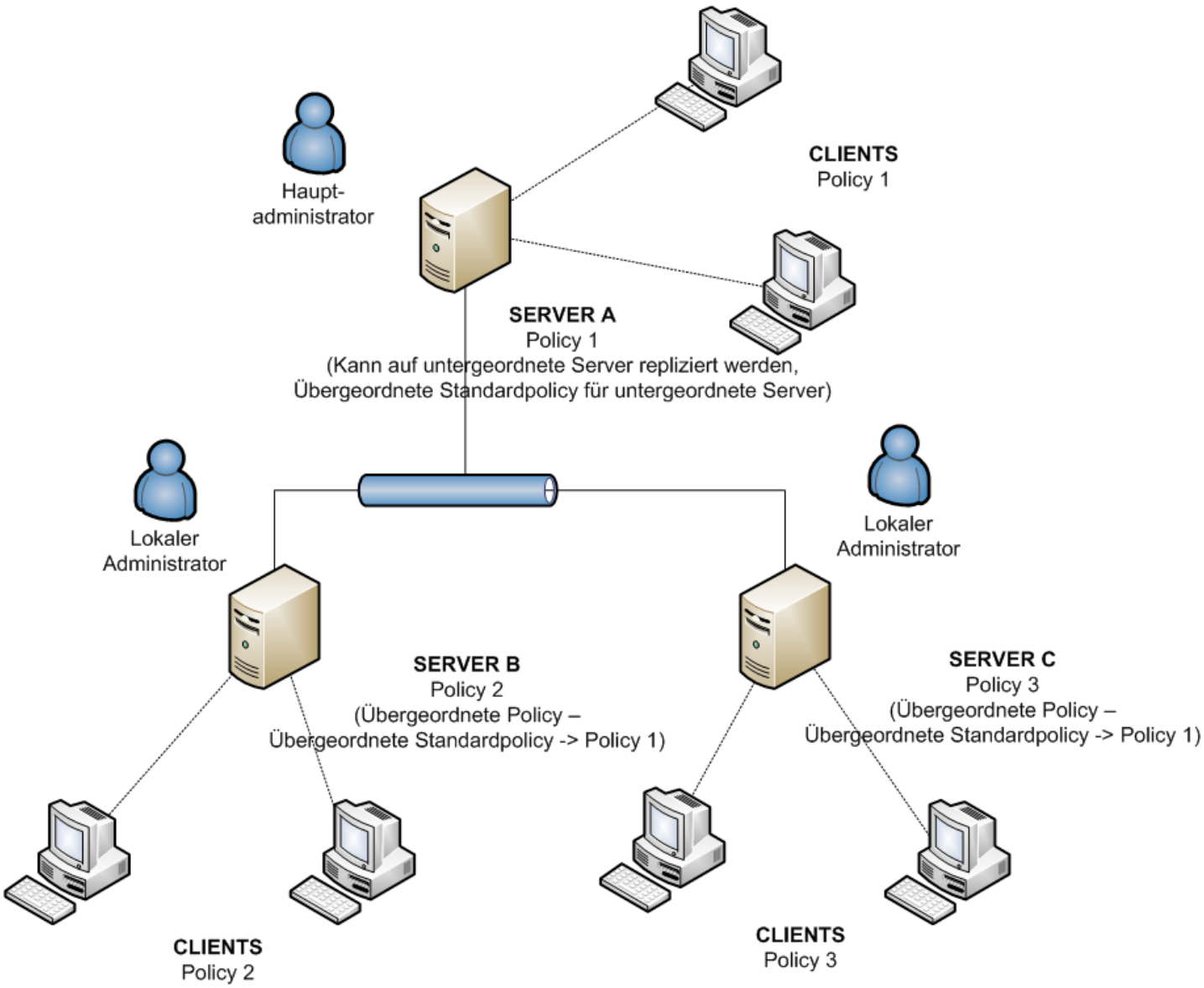
5.3.10.1 Nur Standalone-Server, Policies werden lokal definiert

In diesem Szenario gehen wir von einem kleinen Netzwerk mit einem Hauptserver und zwei untergeordneten Servern aus. Jeder Server hat mehrere Clients. Auf jedem Server ist mindestens eine Policy definiert. Die untergeordneten Server befinden sich in den Zweigniederlassungen des Unternehmens und werden jeweils von einem Administrator vor Ort verwaltet. Jeder Administrator entscheidet für „seinen" Server eigenverantwortlich, welche Policies welchen Clients zugewiesen werden. Der Administrator des Hauptservers greift nicht in diese Konfiguration ein und weist den Clients der untergeordneten Server selbst keine Policies zu. Mit Blick auf die Serverpolicies bedeutet dies, dass Server A keine **Standardpolicy für untergeordnete Server** hat. Außerdem bedeutet es, dass auf Server B und Server C als übergeordnete Policy entweder „Nicht verfügbar" oder eine andere lokale Policy (außer der **übergeordneten Standardpolicy**) eingestellt ist. (Den Servern B und C werden also keine übergeordneten Policies vom übergeordneten Server zugewiesen.)


Haupt-
administrator
CLIENTS
Policy 1
SERVER A
Policy 1,
Policy 2,
...
Lokaler
Administrator
Lokaler
Administrator
SERVER B
Policy 3 (Übergeordnete Policy – N/A),
Policy 4 (Übergeordnete Policy – N/A),
...
SERVER C
Policy 5 (Übergeordnete Policy – N/A),
Policy 6 (Übergeordnete Policy – N/A),
...
CLIENTS
Policy 4
CLIENTS
Policy 5

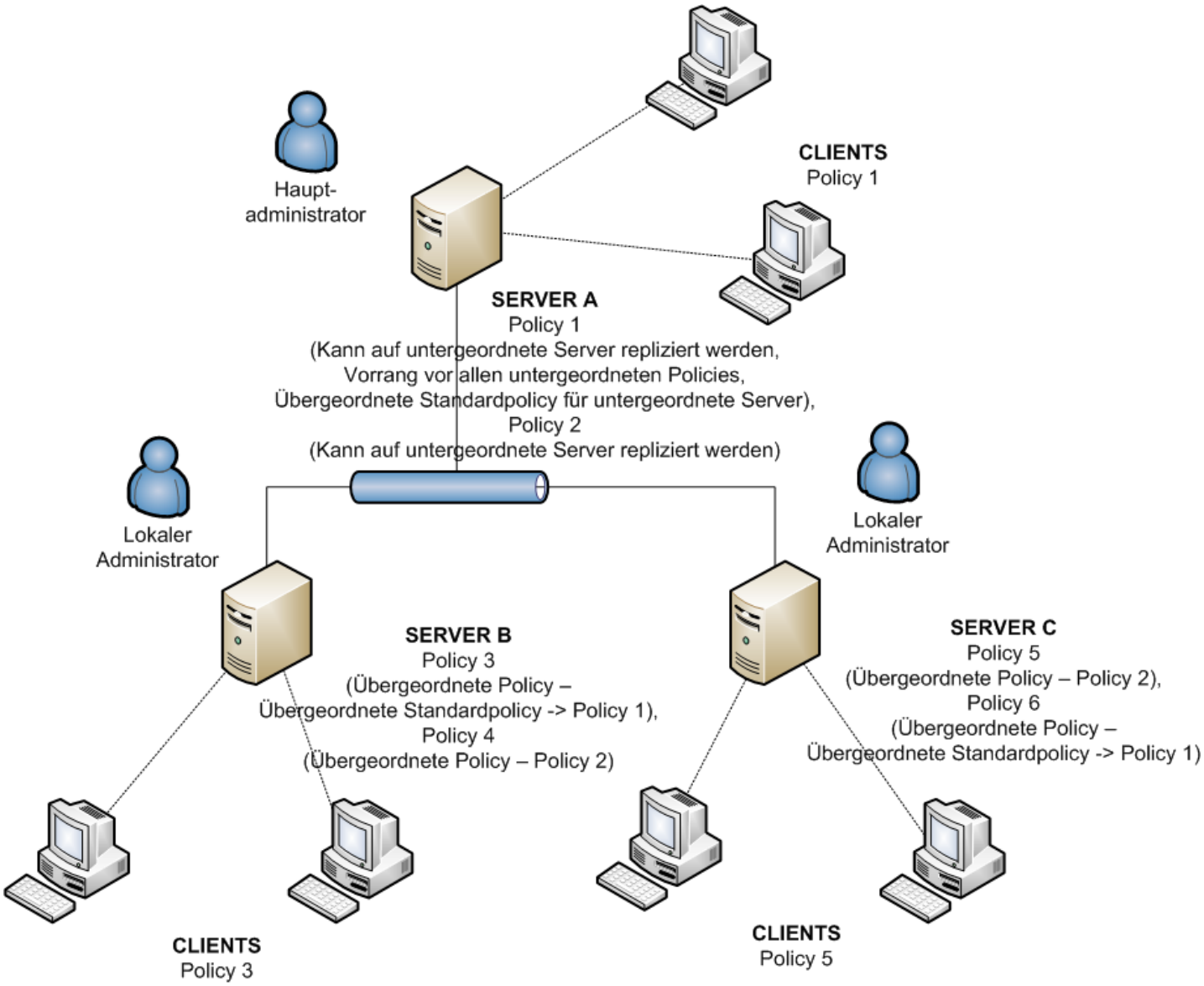
5.3.10.2 Jeder Server wird einzeln administriert - Policies werden lokal verwaltet, aber die übergeordnete Standardpolicy wird vom übergeordneten Server geerbt

Die Konfiguration aus dem vorherigen Szenario gilt auch für dieses Szenario. Auf Server A ist diesmal jedoch eine Standardpolicy für untergeordnete Server aktiviert. Die untergeordneten Server erben dadurch die Konfiguration der übergeordneten Standardpolicy vom Master-Server. In diesem Szenario konfigurieren die Administratoren der lokalen Server ihre Policies weitgehend eigenständig. Die Policies auf den untergeordneten Servern erben zwar die übergeordnete Standardpolicy, die lokalen Administratoren können diese jedoch mit eigenen Policies anpassen.



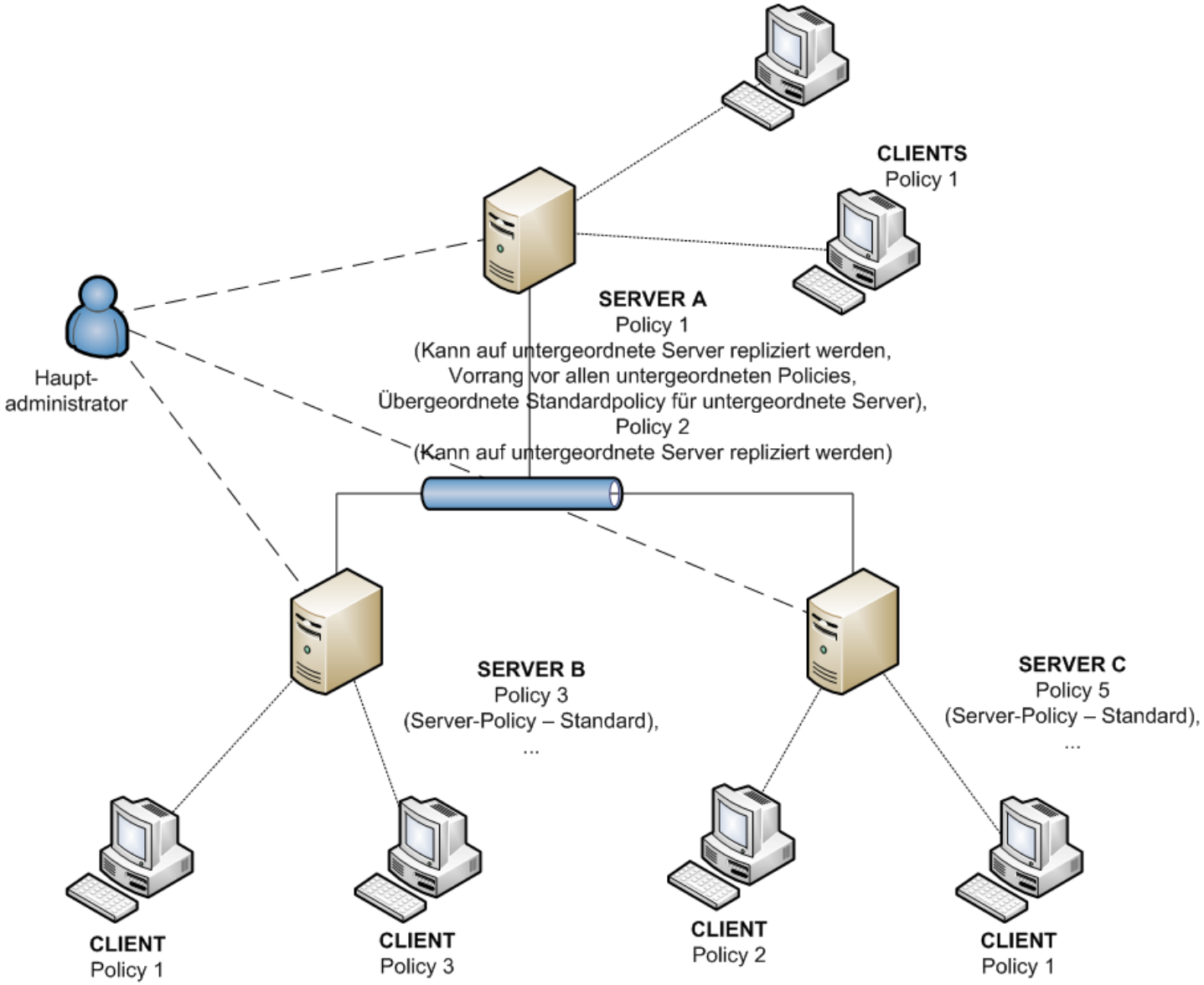
5.3.10.3 Vererbung von Policies durch einen übergeordneten Server

Für dieses Szenario gilt dasselbe Netzwerkmodell wie in den vorhergehenden beiden Szenarien. Zusätzlich enthält der Master-Server neben der übergeordneten Standardpolicy weitere Policies, die auf die untergeordneten Server repliziert werden und dort als übergeordnete Policies dienen. In der Policy 1 (siehe Abbildung unten) ist die Option **Vorrang vor allen untergeordneten Policies** aktiviert. Der Administrator des lokalen Servers hat dadurch weiterhin weitreichenden Handlungsspielraum. Welche Policies auf die untergeordneten Server repliziert werden und dort als übergeordnete Policies dienen, entscheidet jedoch der Administrator des Master-Servers. Durch die Einstellung **Vorrang vor allen...** ist festgelegt, dass die Konfigurationen der ausgewählten Policies Vorrang vor den Konfigurationen haben, die auf den lokalen Servern definiert sind.



5.3.10.4 Zuweisung von Policies ausschließlich vom übergeordneten Server

Dieses Szenario steht für eine zentralisierte Policyverwaltung. Policies für die Clients werden ausschließlich auf dem zentralen Server erstellt, bearbeitet und zugewiesen. Lokale Administratoren sind nicht berechtigt, sie zu ändern. Auf allen untergeordneten Servern ist nur eine einzige leere Basispolicy vorhanden (standardmäßig unter dem Namen „Server-Policy"). Diese Policy dient als übergeordnete Standardpolicy für primäre Clients.



5.3.10.5 Zuweisung über Policyregeln

In unserem nächsten Beispiel werden Policies automatisch mithilfe von Policyregeln zugewiesen. Diese Methode ergänzt die bisher beschriebenen Szenarien und soll diese nicht ersetzen, sondern vielmehr in Kombination mit ihnen eingesetzt werden.

Wenn jeder Server von einem lokalen Administrator verwaltet wird, kann jeder dieser Administratoren eigene Policyregeln für „seine" Clients einrichten. In einem solchen Szenario ist darauf zu achten, dass keine Konflikte zwischen den Policyregeln entstehen - etwa wenn der übergeordnete Server einem Client aufgrund einer Policyregel eine bestimmte Policy zuweist, der untergeordnete Server aufgrund seiner eigenen Regeln jedoch eine andere Policy.

Ein zentralisiertes System senkt letztendlich die Konfliktwahrscheinlichkeit deutlich, da die gesamte Verwaltung auf dem zentralen Server stattfindet.

5.3.10.6 Zuweisung an Gruppen

In bestimmten Situationen kann die Zuweisung von Policies an Clientgruppen die bisher beschriebenen Methoden ergänzen. Die Gruppen können Sie entweder von Hand oder über die Funktion **Active Directory-Synchronisierung** erstellen.
Die Aufnahme von Clients in die Gruppen kann dabei manuell (**statische Gruppen**) oder automatisch anhand bestimmter Kriterien (**parametrische Gruppen**) erfolgen. Nähere Informationen finden Sie im Kapitel Gruppen-Manager 53.
Die Zuweisung der Policy an die Clientgruppe können Sie von Hand einmalig im **Policy-Manager** durchführen (**Clients hinzufügen > Hinzufügen (erweitert)**) oder automatisch über **Policyregeln** geschehen lassen.

Ein mögliches Szenario könnte beispielsweise wie folgt aussehen:

Der Administrator möchte Clients aus unterschiedlichen AD-Gruppen unterschiedliche Policies zuweisen. Wenn ein Client in eine andere Gruppe verschoben wird, soll sich auch die zugewiesene Policy automatisch ändern.

1. Zunächst richten Sie hierfür die **Active Directory-Synchronisierung** im **Gruppen-Manager** nach Bedarf ein. Wichtig ist dabei insbesondere die Einstellung des korrekten Intervalls für die Synchronisierung (verfügbare Optionen: stündlich, täglich, wöchentlich, monatlich).
2. Nach der ersten erfolgreichen Synchronisierung werden die AD-Gruppen im Bereich **Statische Gruppen** angezeigt.
3. Erstellen Sie eine neue Policyregel mit der Bedingung **ERA-Gruppen IN** und/oder **ERA-Gruppen NOT IN**.
4. Legen Sie die Gruppen fest, die Sie mit dieser Bedingung verknüpfen möchten.
5. Geben Sie nun an, welche Policy den Clients zugewiesen werden soll, die die Regelbedingung(en) erfüllen, und klicken Sie auf **OK**, um die Regel zu speichern.

HINWEIS: Statt den Schritten 3 bis 5 können Sie auch den **Assistenten für Policyregeln** verwenden, um auf der Grundlage der vorhandenen Gruppenstruktur eine passende Policystruktur zu erstellen und die neuen Policies über entsprechende Regeln den Gruppen zuzuweisen.

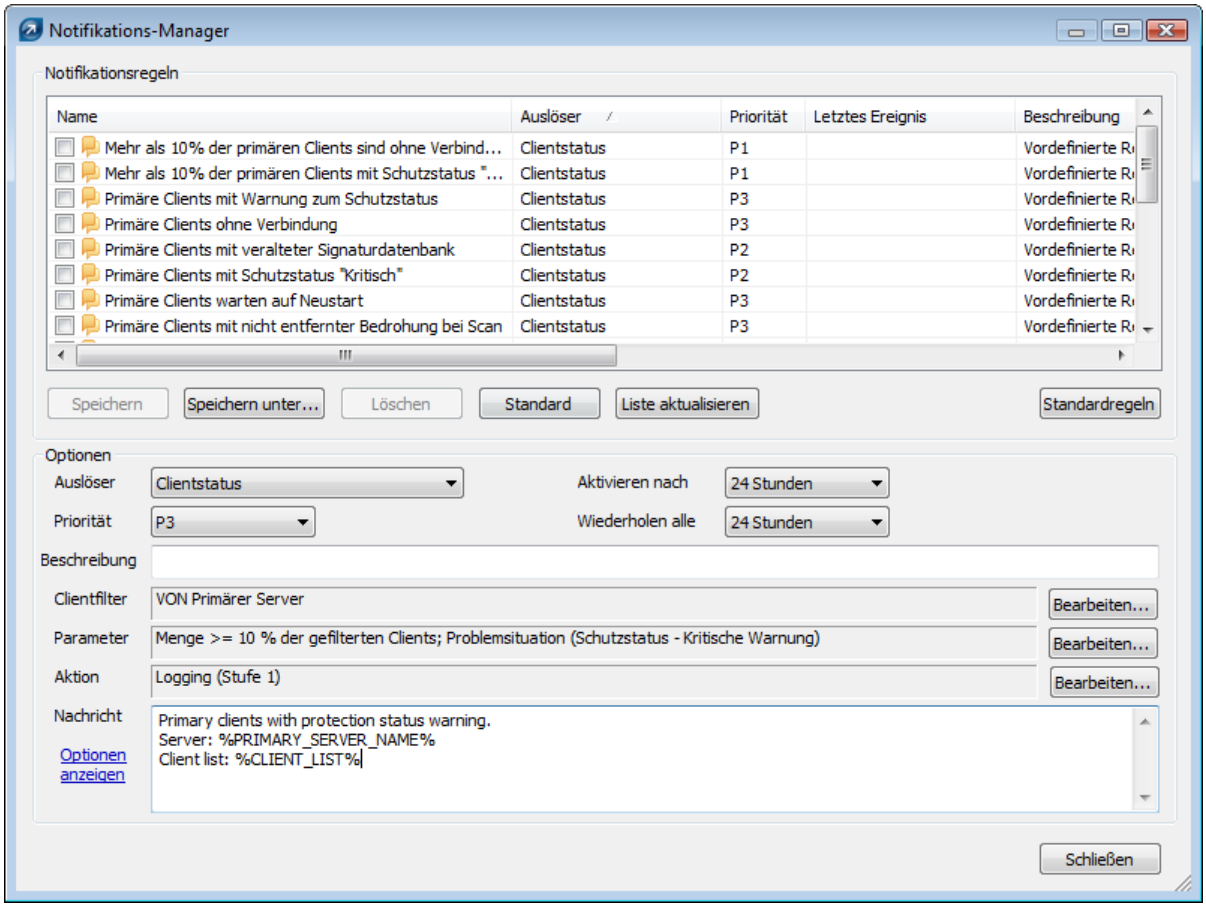
Auf diese Weise können Sie eine passende Policyregel für jede AD-Gruppe definieren. Welche Policy einem bestimmten Client zugewiesen wird, richtet sich nun danach, welcher AD-Gruppe er angehört. Da eine regelmäßige AD-Synchronisierung eingerichtet wurde, werden Änderungen an der AD-Gruppenmitgliedschaft des Clients erkannt und bei der Zuweisung der Policy berücksichtigt. Die Policies werden den Clients also automatisch je nach ihrer AD-Gruppe zugewiesen. Sobald die Regeln und Policies erst einmal komplett definiert sind, geschieht die Zuweisung der Policies automatisch und ohne Eingriffe des Administrators.
Der große Vorteil eines solchen Ansatzes ist die direkte, automatische Verknüpfung zwischen der AD-Gruppenmitgliedschaft und der zugewiesenen Policy.

5.4 Notifikationen

Um die Sicherheit und Integrität eines Netzwerks zu gewährleisten, muss es möglich sein, System- und Netzwerkadministratoren beim Auftreten von wichtigen Ereignissen durch eine entsprechende Benachrichtigung (Notifikation) zu informieren. Eine frühzeitige Warnung bei einem Fehler oder bei Aktivitäten eines Schadprogramms kann den Zeit- und Kostenaufwand zur Behebung des Problems deutlich reduzieren. Die nächsten drei Abschnitte geben einen Überblick über die Benachrichtigungsmöglichkeiten in ERA.

5.4.1 Notifikations-Manager

Um das Hauptfenster des **Notifikations-Managers** zu öffnen, klicken Sie auf **Extras** > **Notifikations-Manager**.



Das Hauptfenster gliedert sich in zwei Bereiche. Der Abschnitt **Notifikationsregeln** im oberen Teil des Fensters enthält eine Liste der vorhandenen Regeln (sowohl vordefinierte als auch vom Benutzer erstellte). Damit eine hier aufgeführte Regel tatsächlich zum Erzeugen von Notifikationen verwendet wird, muss ihr Kontrollkästchen aktiviert sein. Standardmäßig sind keine Notifikationen aktiviert. Prüfen Sie daher immer, ob die gewünschten Regeln tatsächlich aktiv sind.

Mit den Schaltflächen unter der Regelliste können Sie verschiedene Aktionen ausführen: **Speichern** (Änderungen an einer Regel speichern), **Speichern unter** (geänderte Regel unter einem neuen Namen speichern), **Löschen**, **Standard** (Standardeinstellungen für den ausgewählten Auslöser wiederherstellen), **Liste aktualisieren** sowie **Standardregeln** (Standardregeln in der Liste wiederherstellen).

Der Bereich **Optionen** in der unteren Hälfte des Fensters zeigt die Einstellungen der aktuell ausgewählten Regel. Alle Felder und Optionen in diesem Bereich werden anhand der Beispielregel aus dem Kapitel Erstellen von Regeln 72 beschrieben.

Für jede Regel können Sie die Kriterien angeben, bei denen die Regel aktiviert wird - den so genannten „Auslöser". Die folgenden Auslösertypen stehen zur Verfügung:

- **Clientstatus** - Die Regel wird ausgelöst, wenn auf einem oder mehreren Clients ein Problem vorliegt.
- **Serverstatus** - Die Regel wird ausgelöst, wenn auf einem oder mehreren Servern ein Problem vorliegt.
- **Ereignis „Abgeschlossener Task"** - Die Regel wird ausgelöst, nachdem der angegebene Task abgeschlossen wurde.
- **Ereignis „Neuer Client"** - Die Regel wird ausgelöst, sobald eine neue Clientverbindung für den Server vorliegt (gilt auch für replizierte Clients).
- **Ereignis „Neues Log"** - Die Regel wird ausgelöst, wenn das angegebene Ereignis in einem der Logs gefunden wird.

Je nach Typ des Auslösers können Sie weitere Optionen für die Regeln aktivieren oder deaktivieren. Beim Erstellen einer neuen Regel sollten Sie daher als erstes den Auslösertyp festlegen.

Mit der Liste **Priorität** können Sie die Priorität der Regel festlegen. **P1** ist die höchste, **P5** die niedrigste Priorität. Die Priorität hat keinerlei Auswirkung auf die Funktion der Regeln. Sie können die Priorität in den Benachrichtigungstext

aufnehmen, indem Sie die Variable *%PRIORITY%* verwenden. Unter der Liste **Priorität** finden Sie das Feld **Beschreibung** . Es empfiehlt sich, jeder Regel eine aussagefähige Beschreibung zu geben, z. B. *„Regel für Warnungen bei erkannten Bedrohungen"*.

Sobald das System feststellt, dass die Auslösebedingungen für die Regel bei einem oder mehreren Clients erfüllt sind, wird ein Clientfilter angewendet. Einen solchen Filter können Sie für jede Regel definieren, bei der Clients involviert sind. Zum Einrichten des Clientfilters klicken Sie im Bereich **Clientfilter** auf **Bearbeiten**. Legen Sie im daraufhin erscheinenden Dialogfenster die Einstellungen für den Clientfilter fest. Bei der Ausführung der Regel werden dann nur diejenigen Clients berücksichtigt, die die Kriterien des Clientfilters erfüllen. Die folgenden Filterkriterien stehen zur Verfügung:

- **VON Primärer Server** - Nur Clients vom primären Server (kann mit der Option NICHT VON auch umgekehrt werden)
- **Primärer Server IN** - Primärer Server wird in die Ausgabe aufgenommen
- **HAT Markierung „Neu"** - Nur Clients mit der Markierung *„Neu"* (kann mit der Option HAS NOT auch umgekehrt werden)
- **ERA-Gruppen IN** - Nur Clients, die der angegebenen Gruppe angehören
- **Domäne/Arbeitsgruppe IN** - Nur Clients, die der angegebenen Domäne angehören
- **Maske für Computernamen IN** - Nur Clients mit dem festgelegten Computernamen
- **HAT IP-Maske** - Nur Clients innerhalb der angegebenen IP-Maske
- **HAT IP-Bereich** - Nur Clients im angegebenen IP-Adressbereich
- **HAT Festgelegte Policy** - Nur Clients, denen die angegebene Policy zugewiesen wurde (kann mit der Option HAS NOT auch umgekehrt werden)

Wenn Sie den Clientfilter für Ihre Notifikationsregel eingerichtet haben, klicken Sie auf **OK**. Konfigurieren Sie nun die Parameter für die Regel. Diese Clientparameter legen fest, welche Kriterien ein Client oder eine Gruppe von Clients erfüllen muss, damit die festgelegte Notifikationsaktion ausgeführt wird. Um die verfügbaren Parameter anzuzeigen, klicken Sie im Bereich **Parameter** auf **Bearbeiten**.

Welche Parameter zur Verfügung stehen, hängt vom ausgewählten Auslösertyp ab. Im Folgenden finden Sie eine Liste aller Parameter, die für jeden Auslösertyp zur Verfügung stehen.

Für den Auslösertyp „Clientstatus" stehen die folgenden Parameter zur Verfügung:

- **Schutzstatus - Beliebige Warnung** - Spalte „Schutzstatus" enthält eine beliebige Warnung
- **Schutzstatus - Kritische Warnung** - Spalte „Schutzstatus" enthält eine kritische Warnung
- **Signaturdatenbank-Version** - Problem mit der Signaturdatenbank (sechs mögliche Werte)
    - **Vorgängerversion** - Signaturdatenbank liegt eine Version hinter der aktuellen Version zurück
    - **Ältere Version oder nicht verfügbar** - Signaturdatenbank liegt mehr als eine Version hinter der aktuellen Version zurück
    - **Älter als 5 Versionen oder nicht verfügbar** - Signaturdatenbank liegt mehr als fünf Versionen hinter der aktuellen Version zurück
    - **Älter als 10 Versionen oder nicht verfügbar** - Signaturdatenbank liegt mehr als zehn Versionen hinter der aktuellen Version zurück
    - **Älter als 7 Tage oder nicht verfügbar** - Signaturdatenbank liegt mehr als 7 Tage hinter der aktuellen Version zurück
    - **Älter als 14 Tage oder nicht verfügbar** - Signaturdatenbank liegt mehr als 14 Tage hinter der aktuellen Version zurück

- **Warnung wegen überfälliger Verbindung** - Im angegebenen Zeitraum wurde keine Verbindung aufgebaut.
- **Letzte Bedrohungswarnung** - Die Spalte „Letzte Bedrohungswarnung" enthält eine Bedrohungswarnung.
- **Letztes Ereignis** - Die Spalte „Letzte Ereigniswarnung" enthält einen Eintrag.
- **Letzte Firewall-Warnung** - Die Spalte „Letzte Firewall-Warnung" enthält eine Warnung zu einem Firewall-Ereignis.
- **Markierung „Neu"** - Für den Client ist die Markierung „Neu" aktiviert.
- **Im Zustand „Warten auf Neustart"** - Der Client wartet auf einen Neustart.
- **Bedrohung bei letztem Scan gefunden** - Beim letzten Scan wurde die angegebene Anzahl von Bedrohungen auf dem Client gefunden.
- **Bedrohung bei letztem Scan nicht entfernt** - Beim letzten Scan wurde die angegebene Anzahl von Bedrohungen nicht vom Client entfernt.

Alle Parameter können umgekehrt werden, nicht alle dieser Umkehrungen sind jedoch auch sinnvoll. Eine Umkehrung eignet sich nur für Parameter, die einen Binärwert überprüfen, der entweder wahr oder falsch sein kann. Der Parameter **HAT Markierung „Neu"** ist beispielsweise nur bei Clients erfüllt, bei denen die Markierung *„Neu"* gesetzt ist. Die Umkehrung dieses Parameters wäre dementsprechend bei allen Clients erfüllt, bei denen diese Markierung nicht gesetzt ist.

Alle oben genannten Bedingungen können logisch miteinander verknüpft und umgekehrt werden. Über die Option **Die Regel wird angewendet, wenn** können Sie eine der beiden folgenden Verknüpfungsarten wählen:

- **alle Bedingungen erfüllt sind** - Die Regel wird nur dann ausgeführt, wenn **alle** angegebenen Bedingungen erfüllt sind.
- **eine der Bedingungen erfüllt ist** - Die Regel wird ausgeführt, wenn mindestens **eine** der angegebenen Bedingungen erfüllt ist.

Für den Auslösertyp „Serverstatus" stehen die folgenden Parameter zur Verfügung:

- **Server-Update** - Server ist auf dem neuesten Stand.

- **Kein Server-Update seit** - Im angegebenen Zeitraum hat kein Server-Update stattgefunden.

- **Serverlog** - Das Serverlog enthält einen Eintrag der folgenden Typen:

  - **Fehler** - Fehlermeldungen
  - **Fehler + Warnungen** - Fehler- und Warnmeldungen
  - **Fehler + Warnungen + Info (Inhaltsstufe 2)** - Fehler-, Warn- und Informationsmeldungen
  - **Log-Einträge nach Typ filtern** - Aktivieren Sie diese Option, um das Serverlog gezielt auf bestimmte Fehler- und Warnmeldungen zu überwachen. Bitte beachten Sie, dass der Log-Umfang in diesem Fall auf die entsprechende Inhaltsstufe gesetzt sein muss (**Extras > Serveroptionen > Logging**), damit die Notifikation wie beabsichtigt funktioniert. Anderenfalls findet die Regel im Serverlog nie eine Meldung, die eine Notifikation auslösen würde. Die folgenden Log-Typen stehen zur Verfügung:

- **ADSI_SYNCHRONIZE** - Active Directory-Gruppensynchronisierung
- **CLEANUP** - Server-Löschläufe
- **CREATEREPORT** - Erstellen von Berichten auf Abruf
- **DEINIT** - Server wird heruntergefahren
- **INIT** - Server wird gestartet
- **INTERNAL 1** - Interne Servermeldung
- **INTERNAL 2** - Interne Servermeldung
- **LICENSE** - Lizenzverwaltung
- **MAINTENANCE** - Server-Wartungstasks
- **NOTIFICATION** - Verwaltung von Notifikationen
- **PUSHINST** - Push-Installation
- **RENAME** - Umbenennung von internen Strukturen
- **REPLICATION** - Serverreplikation
- **POLICY** - Verwaltung von Policies
- **POLICYRULES** - Policyregeln
- **SCHEDREPORT** - Automatisch erstellte Berichte
- **SERVERMGR** - Internes Thread-Management des Servers
- **SESSION** - Server-Netzwerkverbindungen
- **SESSION_USERACTION** - Verschiedene Benutzeraktionen
- **THREATSENSE** - ThreatSense.Net - Einreichen von statistischen Informationen
- **UPDATER** - Server-Update und Erstellen von Mirror-Kopien

Ein Beispiel für einen hilfreichen Parameter ist der Log-Typ UPDATER, mit dem Sie eine Notifikation auslösen können, wenn im Serverlog ein Problem im Zusammenhang mit einem Update oder der Erstellung von Mirror-Kopien gemeldet wird.

- **Lizenzablauf** - Die Lizenz läuft in der angegebenen Anzahl von Tagen ab oder ist bereits abgelaufen. Wenn Sie die Option **Nur warnen, wenn dadurch die Anzahl der Clients in der Lizenz unter die Anzahl der vorhandenen Clients in der Serverdatenbank fallen würde** aktivieren, erfolgt die Notifikation nur, wenn durch den Ablauf der Lizenz die Anzahl der lizenzierten Clients unter die Anzahl der momentan verbundenen Clients fallen würde.

- **Lizenzlimit** - Der Anteil der noch für neue Clients verfügbaren Lizenzen fällt unter den eingestellten Prozentwert.

Für den Auslösertyp „Ereignis Neues Log" stehen die folgenden Parameter zur Verfügung:
- **Log-Typ** - Wählen Sie entweder „Ereignis-Log", „Bedrohungs-Log" oder „Firewall-Log".
- **Log-Stufe** - Stufe des Eintrags im jeweiligen Log
  - Stufe 1 - Kritische Warnungen - Nur kritische Fehler

- **Stufe 2 - wie oben + Warnung** - Wie 1 plus Warnmeldungen
- **Stufe 3 - wie oben + Normal** - Wie 2 plus Informationsmeldungen
- **Stufe 4 - wie oben + Diagnose** - Wie 3 plus Diagnosemeldungen

- **1000 Fälle in 60 Minuten** - Geben Sie an, wie oft die betreffende Meldung in einem bestimmten Zeitraum auftreten muss, damit die Notifikation erfolgt. Standardmäßig sind 1000 Fälle innerhalb einer Stunde eingestellt.

- **Menge** - Anzahl der Clients (absolut oder in Prozent)

Für die anderen Auslösertypen sind keine besonderen Parameter vorhanden.

Wenn die festgelegten Kriterien für eine Regel erfüllt sind, wird automatisch die angegebene Aktion ausgeführt. Um die Aktionen zu konfigurieren, klicken Sie im Bereich **Aktion** auf **Bearbeiten**. Im Aktionseditor stehen die folgenden Optionen zur Verfügung:

- **E-Mail versenden** - Der in der Regel hinterlegte Benachrichtigungstext wird an die angegebene E-Mail-Adresse verschickt. Geben Sie im Feld **Betreff** die Betreffzeile an. Klicken Sie auf **An**, um das Adressbuch zu öffnen.
- **SNMP-Trap** - Es wird eine SNMP-Notifikation erzeugt und verschickt.
- **Befehl ausführen (auf dem Server)** - Der angegebene Befehl wird auf dem Server ausgeführt (z. B. Starten eines Programms).
- **Logging in Datei (auf dem Server)** - Es werden Log-Einträge in die angegebene Log-Datei geschrieben. Über die Liste **Umfang** können Sie den Umfang dieser Einträge festlegen.
- **Auch Nachricht in Log schreiben** - Bewirkt, dass auch der Nachrichtentext ins Log geschrieben wird.
- **Logging in Syslog** - Die Notifikationen werden in die Systemlogs geschrieben. Über die Liste **Umfang** können Sie den Umfang festlegen.
- **Logging** - Die Notifikationen werden ins Serverlog geschrieben. Über die Liste **Umfang** können Sie den Umfang festlegen. Damit diese Option ordnungsgemäß funktioniert, müssen Sie das Logging in ERA Server aktivieren (**Extras** > **Serveroptionen** > **Logging**).

Über das Feld **Nachricht** im unteren Teil des Notifikations-Managers können Sie Format und Inhalt der Notifikation festlegen. Über dynamische Variablen können Sie auch Programm- und Ereignisdaten in den Text einfügen. Verwenden Sie dazu die folgende Syntax: *%VARIABLENNAME%*. Für eine Liste der verfügbaren Variablen klicken Sie auf **Optionen anzeigen**.

- **Server_Last_Updated** - Letztes Update des Servers
- **Primary_Server_Name**
- **Rule_Name**
- **Rule_Description**
- **Client_Filter** - Einstellungen des Clientfilters
- **Client_Filter_Short** - Einstellungen des Clientfilters in Kurzform
- **Client_List** - Liste der Clients
- **Triggered** - Datum der letzten Notifikation (ohne Wiederholungen)
- **Triggered_Last** - Datum der letzten Notifikation (einschließlich Wiederholungen)
- **Priority** - Priorität der Notifikationsregel
- **Log_Text_Truncated** - Log-Text, der die Notifikation ausgelöst hat (abgeschnitten)
- **Task_Result_List** - Liste der abgeschlossenen Tasks
- **Parameters** - Parameter der Regel
- **Last_Log_Date** - Datum des letzten Logs
- **License_Info_Merged** - Lizenzinformationen (Zusammenfassung)
- **License_Info_Full** - Lizenzinformationen (komplett)
- **License_Days_To_Expiry** - Tage bis zum Ablauf
- **License_Expiration_Date** - Nächstes Ablaufdatum
- **License_Clients_Left** - Noch verfügbare Client-Verbindungslizenzen in der aktuellen Lizenz
- **License_Customer** - Lizenznehmer/Kunde (zusammengeführt)
- **Actual_License_Count** - Anzahl der Clients, die momentan mit dem Server verbunden sind
- **Virus_Signature_DB_Version** - Aktuelle Version der Signaturdatenbank
- **Pcu_List** - Aktuelle Liste der Programmkomponenten-Updates (PCUs)

Als letzte Einstellung legen Sie noch den Ausführungszeitpunkt fest. Bevor die Regel ausgeführt wird, kann zunächst eine bestimmte Zeit lang gewartet werden (eine Stunde bis drei Monate). Wenn die Regel baldmöglichst ausgeführt werden soll, wählen Sie in der Liste **Aktivieren nach** den Eintrag **Baldmöglichst**. Die Notifikationsregeln werden standardmäßig alle zehn Minuten überprüft. Mit der Einstellung **Baldmöglichst** sollte die Regel also spätestens zehn

Minuten nach Eintreten des Auslöseereignisses ausgeführt werden. Wenn Sie eine andere Zeitspanne auswählen, wird die Aktion automatisch nach Ablauf dieser Zeitspanne ausgeführt (sofern die Kriterien der Regel erfüllt sind).

Über die Liste **Wiederholen alle ...** können Sie ein Zeitintervall festlegen, in dem die Aktion wiederholt werden soll. Die Aktion wird allerdings nur dann wiederholt, wenn die Auslösekriterien der Regel zum betreffenden Zeitpunkt noch erfüllt sind. Über die Einstellung **Serveroptionen** > **Erweitert** > **Erweiterte Einstellungen bearbeiten** > **ESET Remote Administrator** > **ERA Server** > **Einstellungen** > **Notifikation** > **Intervall für die Verarbeitung von Notifikationen (Minuten)** können Sie festlegen, in welchem Zeitintervall der Server die aktiven Regeln überprüft und ausführt.

Der Standardwert ist 10 Minuten. Ein niedrigerer Wert wird nicht empfohlen, da dies die Serverleistung deutlich beeinträchtigen kann.

Der Notifikations-Manager enthält standardmäßig eine Reihe vordefinierter Regeln. Um eine Regel zu aktivieren, aktivieren Sie das dazugehörige Kontrollkästchen. Die folgenden Notifikationsregeln stehen zur Verfügung. Wenn sie aktiviert werden und die entsprechenden Auslöserkriterien erfüllt sind, werden Log-Einträge erzeugt.

- **Mehr als 10% der primären Clients sind ohne Verbindung** - Wenn mehr als 10 % der Clients mindestens eine Woche lang keine Verbindung zum Server aufgebaut haben, wird die Regel baldmöglichst ausgeführt.
- **Mehr als 10% der primären Clients mit Schutzstatus „Kritisch"** - Wenn mehr als 10 % der Clients eine kritische Warnung zum Schutzstatus gemeldet und mindestens eine Woche lang keine Verbindung zum Server aufgebaut haben, wird die Regel baldmöglichst ausgeführt.
- **Primäre Clients mit Warnung zum Schutzstatus** - Regel wird ausgeführt, wenn bei mindestens einem Client eine Warnung zum Schutzstatus vorliegt und der Client mindestens eine Woche lang keine Verbindung zum Server aufgebaut hat.
- **Primäre Clients ohne Verbindung** - Regel wird ausgeführt, wenn mindestens ein Client mindestens eine Woche lang keine Verbindung zum Server aufgebaut hat.
- **Primäre Clients mit veralteter Signaturdatenbank** - Regel wird ausgeführt, wenn die Version der Signaturdatenbank auf einem Client mindestens zwei Versionen hinter der aktuellen Version liegt und der Client innerhalb der letzten sieben Tage mindestens einmal mit dem Server verbunden war.
- **Primäre Clients mit Schutzstatus „Kritisch"** - Regel wird ausgeführt, wenn auf einem Client eine kritische Warnung zum Schutzstatus vorliegt und der Client innerhalb der letzten sieben Tage mindestens einmal mit dem Server verbunden war.
- **Primäre Clients mit neuerer Signaturdatenbank als auf dem Server** - Regel wird ausgeführt, wenn ein Client eine neuere Version der Signaturdatenbank als auf dem Server verwendet und innerhalb der letzten sieben Tage mindestens einmal mit dem Server verbunden war.
- **Primäre Clients warten auf Neustart** - Regel wird ausgeführt, wenn ein Client auf einen Neustart wartet und innerhalb der letzten sieben Tage mindestens einmal mit dem Server verbunden war.
- **Primäre Clients mit nicht entfernter Bedrohung bei Scan** - Regel wird baldmöglichst ausgeführt, wenn mindestens eine Bedrohung bei einem Scan auf einem Client nicht entfernt werden konnte und der Client innerhalb der letzten sieben Tage mindestens einmal mit dem Server verbunden war.
- **Task abgeschlossen** - Regel wird baldmöglichst ausgeführt, wenn ein Task auf einem Client abgeschlossen wurde.
- **Neue primäre Clients** - Regel wird baldmöglichst ausgeführt, wenn ein neuer Client eine Verbindung zum Server aufgebaut hat.
- **Neue replizierte Clients** - Regel wird nach einer Stunde ausgeführt, wenn ein neuer replizierter Client in die Clientliste aufgenommen wurde.
- **Möglicher Virenausbruch** - Regel wird ausgeführt, wenn auf mindestens 10 % der Clients innerhalb von einer Stunde jeweils mehr als 1000 kritische Warnungen ins Bedrohungs-Log geschrieben werden.
- **Möglicher Angriff über das Netzwerk** - Regel wird ausgeführt, wenn auf mindestens 10 % der Clients innerhalb von einer Stunde jeweils mehr als 1000 kritische Warnungen ins Log der ESET Personal Firewall geschrieben werden.
- **Server-Update abgeschlossen** - Regel wird ausgeführt, wenn ein Server-Update abgeschlossen wurde.
- **Server nicht aktualisiert** - Regel wird baldmöglichst ausgeführt, wenn auf dem Server mindestens fünf Tage lang kein Update stattgefunden hat.
- **Fehler in Server-Textlog** - Regel wird ausgeführt, wenn das Serverlog eine Fehlermeldung enthält.
- **Lizenzablauf** - Regel wird baldmöglichst ausgeführt, wenn die aktuelle Lizenz innerhalb von 20 Tagen abläuft und durch den Ablauf der Lizenz die Anzahl der lizenzierten Clients unter die Anzahl der momentan verbundenen Clients fallen würde.
- **Lizenzlimit** - Regel wird ausgeführt, wenn der Anteil der noch für neue Clients verfügbaren Lizenzen unter 10 % fällt.

Soweit nicht anders angegeben, werden alle Regeln nach 24 Stunden ausgeführt, alle 24 Stunden wiederholt und gelten für den primären Server und primäre Clients.

5.4.1.1 Notifikationen per SNMP-Trap

SNMP (Simple Network Management Protocol) ist ein einfaches, weit verbreitetes Managementprotokoll, das sich insbesondere für die Überwachung und Identifikation von Netzwerkproblemen eignet. Unter anderem umfasst es die Aktion TRAP, mit der sich benutzerdefinierte Daten übertragen lassen. In ERA werden solche TRAP-Pakete zum Versand von Notifikationen verwendet.

Zur Nutzung der Trap-Funktion muss SNMP auf demselben Computer wie ERAS korrekt installiert und konfiguriert sein (**Start** > **Systemsteuerung** > **Software** > **Windows-Komponenten hinzufügen/entfernen**). Der SNMP-Dienst sollte wie im folgenden Artikel beschrieben konfiguriert werden: http://support.microsoft.com/kb/315154. In ERAS müssen Sie außerdem eine SNMP-Notifikationsregel aktivieren. In ERAS müssen Sie außerdem eine SNMP-Notifikationsregel aktivieren.

Die so erzeugten Notifikationen können im SNMP-Manager angezeigt werden. Dieser muss hierzu mit einem SNMP-Server verbunden sein, auf dem die Konfigurationsdatei *eset_ras.mib* importiert wurde. Diese Datei ist standardmäßig in der ERA-Installation enthalten und liegt in der Regel im Ordner *C:\Programme\ESET\ESET Remote Administrator\Server\snmp*.

5.4.2 Erstellen von Regeln

Im Folgenden wird an einem Beispiel gezeigt, wie Sie eine Regel erstellen, die eine E-Mail-Benachrichtigung an den Administrator verschickt, wenn auf einem Client-Arbeitsplatzrechner ein Problem mit dem Schutzstatus vorliegt. Die Benachrichtigung wird außerdem in einer Datei namens *log.txt* gespeichert.

1) Wählen Sie in der Liste **Auslöser** den Eintrag **Clientstatus** aus.

2) Übernehmen Sie die vorgegebenen Werte für die Felder **Priorität, Aktivieren nach** sowie **Wiederholen alle**. Die Regel erhält dann automatisch die Priorität 3 und wird nach 24 Stunden aktiviert.

3) Geben Sie im Feld **Beschreibung** den Text **Schutzstatus-Benachrichtigung für Clients in der Zentrale** ein.

4) Klicken Sie im Bereich **Clientfilter** auf **Bearbeiten** und aktivieren Sie ausschließlich die Bedingung **ERA-Gruppen IN**. Klicken Sie im unteren Teil des Dialogfensters auf den Link **festlegen** und geben Sie im daraufhin erscheinenden Fenster den Wert *Zentrale* ein. Klicken Sie auf **Hinzufügen** und dann zur Bestätigung zweimal auf **OK**. Die Regel wird so nur auf Clients aus der Gruppe „Zentrale" angewendet.

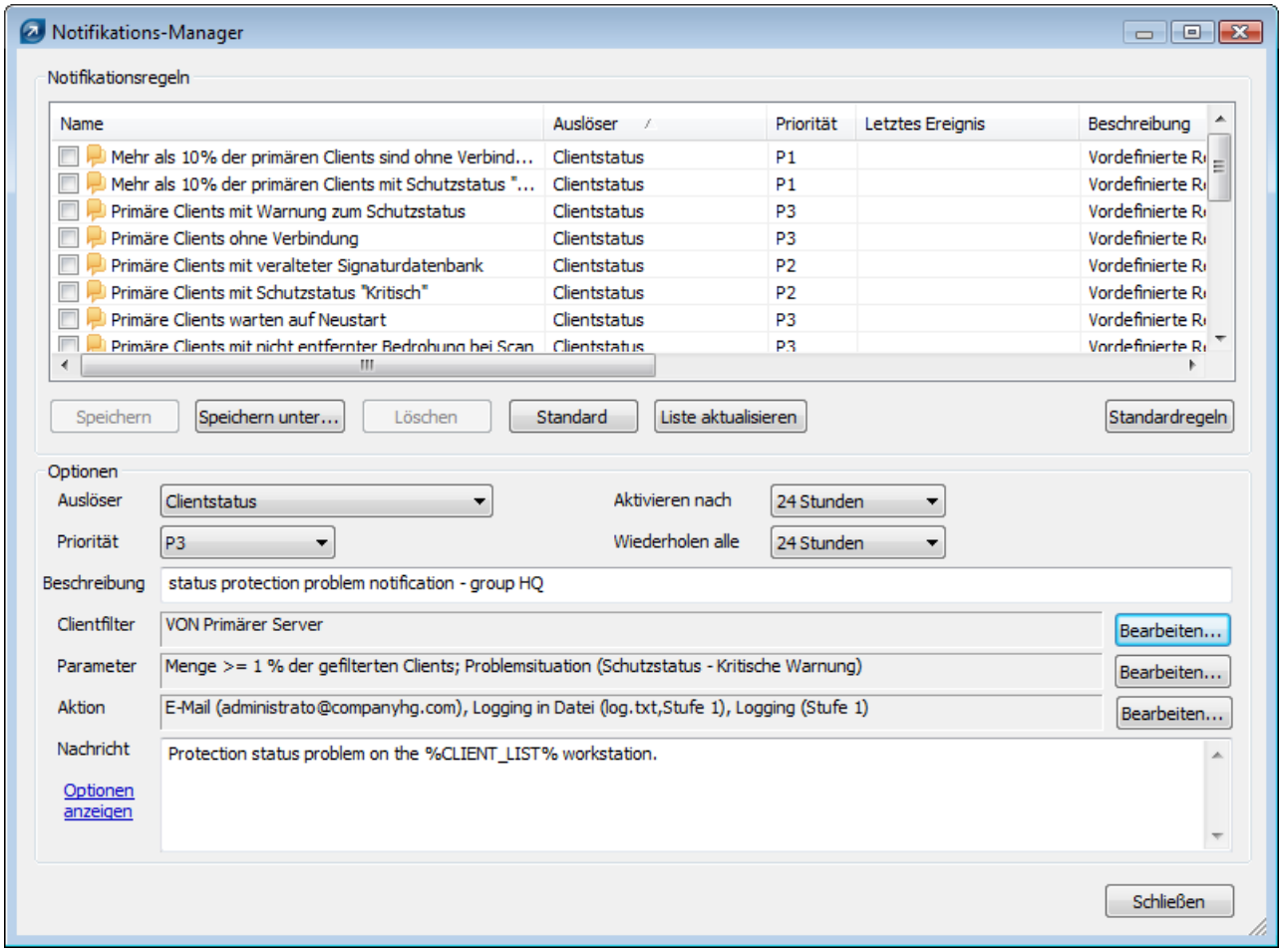
5) Klicken Sie auf **Parameter > Bearbeiten**, um weitere Parameter für die Regel festzulegen. Deaktivieren Sie alle Optionen außer **HAT Schutzstatus - Beliebige Warnung**.

6) Klicken Sie im Bereich **Aktion** auf **Bearbeiten**. Das Dialogfenster **Aktion** wird angezeigt. Aktivieren Sie die Option **E-Mail versenden**, geben Sie die Empfänger an (Schaltfläche **An**) und tragen Sie einen **Betreff** für die E-Mail ein. Aktivieren Sie anschließend das Kontrollkästchen **Logging in Datei** und geben Sie Namen und Pfad der zu erstellenden Log-Datei ein. Bei Bedarf können Sie auch die **Inhalte** der Log-Datei festlegen. Klicken Sie auf **OK**, um die Aktion zu speichern.

7) Tragen Sie abschließend im Feld **Nachricht** den Text ein, der als Text der E-Mail verschickt werden soll, wenn die Regel ausgelöst wird. Beispiel: „*Problem mit Schutzstatus beim Client %CLIENT_LIST%*".

8) Klicken Sie auf **Speichern unter**, geben Sie einen Namen für die Regel ein (z. B. „*Schutzstatus-Probleme*") und aktivieren Sie ihr Kontrollkästchen in der Liste der Notifikationsregeln.

Die fertige Regel sollte wie in der folgenden Abbildung aussehen:



Die Regel ist jetzt aktiv. Sie wird ausgelöst, wenn bei einem Client aus der Gruppe „Zentrale“ ein Problem mit dem Schutzstatus vorliegt. Der angegebene Administrator erhält dann eine E-Mail-Benachrichtigung mit dem Namen des betroffenen Clients. Klicken Sie auf **Schließen**, um den Notifikations-Manager zu schließen.

5.5 Ausführliche Informationen von Clients

Mit ERA können Sie Informationen zu laufenden Prozessen, Autostart-Programmen usw. von den Client-Arbeitsplatzrechnern abrufen. Hierzu verwenden Sie das direkt in ERAS integrierte Tool ESET SysInspector. Neben weiteren hilfreichen Funktionen kann ESET SysInspector eine gründliche Untersuchung des Betriebssystems durchführen und System-Logs erstellen. Um das Programm zu öffnen, klicken Sie im ERAC-Hauptmenü auf **Extras** > **ESET SysInspector**.

Bei Problemen mit einem bestimmten Client können Sie ein ESET SysInspector-Log von diesem Client anfordern. Hierzu klicken Sie auf der Registerkarte **Clients** mit der rechten Maustaste auf den Client und wählen **Daten anfordern > SysInspector-Informationen anfordern**. Logs können nur von Produkten mit einer Version ab 4.0 abgerufen werden; frühere Versionen unterstützen diese Funktion nicht. Ein Fenster mit den folgenden Optionen wird angezeigt:

- **Snapshot erstellen (und Ergebnis-Log auf dem Client speichern)** - Bewirkt, dass eine Kopie des Logs auf dem Clientcomputer gespeichert wird.

- **Vergleich zum letzten Snapshot vor einem bestimmten Zeitpunkt** - Bewirkt, dass ein Vergleichs-Log angezeigt wird (durch Zusammenführen des aktuellen Logs mit einem älteren Log, falls verfügbar). ERA wählt hierzu das letzte Log, das vor dem angegebenen Datum liegt.

Klicken Sie auf **OK**, um die ausgewählten Logs anzufordern und auf dem Server zu speichern. Um die Logs zu öffnen und anzuzeigen, gehen Sie wie folgt vor.

Die ESET SysInspector-Optionen für einzelne Client-Arbeitsplatzrechner finden Sie auf der Registerkarte **SysInspector** im Dialogfeld **Eigenschaften** des Clients. Das Fenster gliedert sich in drei Bereiche. Der obere Bereich zeigt Informationen zu den aktuellen Logs, die vom jeweiligen Client verfügbar sind. Klicken Sie auf **Aktualisieren**, um die jeweils aktuellen Informationen zu laden.

Der mittlere Bereich (**Optionen für Anforderung**) ist fast identisch mit dem Dialogfenster, das beim Anfordern von Logs von einem Client erscheint (siehe oben). Über die Schaltfläche **Anfordern** können Sie ein ESET SysInspector-Log vom betreffenden Client anfordern.

Der untere Bereich umfasst die folgenden Schaltflächen:

- **Anzeigen** - Öffnet das im oberen Bereich angegebene Log direkt in ESET SysInspector.
- **Speichern unter** - Speichert das aktuelle Log in einer Datei. Die Option **Anschließend Datei in ESET SysInspector Viewer anzeigen** bewirkt, dass das Log nach dem Speichern automatisch geöffnet wird (wie beim Klicken auf **Anzeigen**).

Je nach der Größe des Logs und der Übertragungsgeschwindigkeit läuft die Erstellung und Anzeige neuer Logs auf dem lokalen Client in manchen Fällen etwas langsamer ab. Der Zeitstempel des Logs auf der Registerkarte **SysInspector** im Dialogfeld **Eigenschaften** des Clients gibt an, wann das Log an den Server übermittelt wurde.

5.6 Zentrale Quarantäne

Die zentrale Quarantäne ist eine leistungsstarke Funktion, mit der Administratoren Quarantänedateien auf den Clients komfortabel verwalten können. Sie vereinfacht das Anzeigen, Löschen und Wiederherstellen von Quarantänedateien sowie das Definieren von Ausnahmen für zukünftige Scans. Der Zugriff erfolgt über die Registerkarte **Quarantäne** im Hauptfenster der Konsole oder in den Client-Eigenschaften. Die Quarantäneanzeige umfasst vollständige Angaben zu Datei, Name der Bedrohung, Hashwert, Zeitpunkt des ersten und letzten Auftretens, Dateigröße sowie Häufigkeit des Auftretens.

HINWEIS: Bitte beachten Sie, dass in den Feldern **Objektname**, **Dateiname** und **Erweiterung** nur die ersten drei Objekte angezeigt werden. Für ausführlichere Informationen öffnen Sie das Eigenschaften-Dialogfenster, indem Sie entweder **F3** drücken oder auf das ausgewählte Objekt doppelklicken.

Die zentrale Quarantäne bietet Ihnen einen Überblick über die Quarantänedateien, die lokal auf den Clients gespeichert sind. Die einzelnen Dateien können Sie gezielt anfordern. Angeforderte Dateien werden über eine sichere, verschlüsselte Verbindung auf den ERA Server kopiert. Aus Sicherheitsgründen wird die Datei entschlüsselt, wenn sie auf dem Datenträger gespeichert wird. Anleitungen zur Arbeit mit Quarantänedateien finden Sie im Kapitel Task „Aus Quarantäne wiederherstellen/löschen“ 51.

HINWEIS: Zur Nutzung der zentralen Quarantäne muss auf den Clients EAV/ESS 4.2 oder höher installiert sein.

Qu...	Hash	Empfangen	Erstes Auft...	Letztes Auf...	Objektname	Dateiname	Erweiterung	Größe	Grund	Clientanzahl	Zugriffe	Datei
2	d27265074...	Vor 104 Mi...	Vor 11 Tag...	Vor 11 Tag...	https://sec...	eicar_com....	zip	184	Eicar...	1	1	Keine Daten
1	3395856ce...	Vor 104 Mi...	Vor 11 Tag...	Vor 8 Tagen	C:\$RECYC...	$RE949YA.t...	txt, com, ...	68	Eicar...	1	4	Keine Daten

6. Assistent zum Zusammenführen von Firewall-Regeln

Mit dem Assistenten zum Zusammenführen von Firewall-Regeln können Sie die Firewall-Regeln ausgewählter Clients zusammenführen. Diese Funktion ist sehr praktisch, um eine gemeinsame Konfiguration mit allen Firewall-Regeln zu erstellen, die im Trainingsmodus von den Clients erlernt wurden. Diese Konfiguration kann dann über einen Konfigurations-Task an die Clients übermittelt oder mithilfe einer Policy durchgesetzt werden.

Um den Assistenten zu starten, verwenden Sie entweder das Menü **Extras** oder wählen auf der Registerkarte **Clients** die gewünschten Clients aus, klicken mit der rechten Maustaste darauf und wählen dann den entsprechenden Befehl im Kontextmenü. Die ausgewählten Clients werden dann automatisch in den ersten Schritt des Assistenten übernommen.

HINWEIS: Zum erfolgreichen Abschluss dieses Vorgangs muss für alle ausgewählten Clients die aktuelle Konfiguration auf dem Server gespeichert worden sein (entweder durch Anforderung oder per Replikation).

Der Ablauf ist wie folgt: Zunächst wählen Sie die Clients oder Clientgruppen aus, deren Firewall-Regeln zusammengeführt werden sollen. Im nächsten Schritt sehen Sie eine Liste der ausgewählten Clients mitsamt ihrem Konfigurationsstatus. Wenn eine bestimmte Clientkonfigurationen noch nicht auf dem Server verfügbar ist, können Sie sie über die Schaltfläche **Anfordern** anfordern. In den letzten Schritten wählen Sie aus, welche der zusammengeführten Regeln in der Konfiguration verwendet werden sollen, und speichern sie als *.xml*-Datei.

7. Berichte

Über die Registerkarte „Berichte“ können Sie statistische Daten in Grafiken und Diagramme aufbereiten. Neben der Möglichkeit zur grafischen Ausgabe können Sie die Daten auch zur späteren Weiterverarbeitung im *.csv*-Format (Werte mit Trennzeichen) speichern. Standardmäßig speichert ERA die Ausgabe im HTML-Format. Die meisten Berichte zu Bedrohungen und Infektionen werden auf der Grundlage des Bedrohungs-Logs erzeugt.

Zur Auswahl des Darstellungsstils verwenden Sie die Liste **Stil** im Bereich **Bericht**.

ERA bietet eine Reihe von vordefinierten Bericht-Templates. Wählen Sie den gewünschten Bericht in der Liste **Typ** aus:

- **Clients mit den meisten Bedrohungen**
  Zeigt die „aktivsten“ Client-Arbeitsplatzrechner (gemessen an der Anzahl der erkannten Bedrohungen).
- **Benutzer mit den meisten Bedrohungen**
  Zeigt die „aktivsten“ Benutzer (gemessen an der Anzahl der erkannten Bedrohungen).
- **Häufigste Bedrohungen**
  Zeigt die am häufigsten erkannten Bedrohungen.
- **Bedrohungen mit der größten Verbreitung**
  Zeigt eine Liste der häufigsten Bedrohungen gemessen an ihrer Verbreitung.
- **Verlauf der Bedrohungen**
  Ausbreitungsverlauf von Schadprogrammen (Anzahl der Fälle)
- **Verlauf der Bedrohungen im Vergleich**
  Ausbreitungsverlauf bestimmter Bedrohungen (ausgewählt über Filter) im Vergleich zu allen Bedrohungen
- **Bedrohungen nach Scanner**
  Anzahl der Bedrohungswarnungen von den einzelnen Programmkomponenten
- **Bedrohungen nach Objekten**
  Anzahl der Bedrohungswarnungen nach der jeweiligen Angriffsstelle (E-Mails, Dateien, Systembereiche)
- **Kombinierter Bericht: Clients mit den meisten Bedrohungen / Häufigste Bedrohungen**
  Kombination der oben genannten Berichte
- **Kombinierter Bericht: Häufigste Bedrohungen / Verlauf der Bedrohungen**
  Kombination der oben genannten Berichte
- **Kombinierter Bericht: Häufigste Bedrohungen / Verlauf der Bedrohungen im Vergleich**
  Kombination der oben genannten Berichte
- **Clients in Gruppen**
  Zeigt die Anzahl der Clients in den ausgewählten Gruppen
- **Clients in Gruppen - Anteil an Gesamtheit**
  Zeigt den Prozentanteil der Clients in den ausgewählten Gruppen an der Gesamtheit aller Clients
- **Kombinierter Bericht: Clients in Gruppen / Clients**
  Zeigt die Anzahl der Clients in den ausgewählten Gruppen sowie (durch Klicken auf den jeweiligen Gruppennamen) eine Liste der Clients in jeder dieser Gruppen.
- **Clients mit den meisten Angriffen über das Netzwerk**
  Zeigt die Clients mit den meisten Angriffen über das Netzwerk.
- **Häufigste Angriffe über das Netzwerk**
  Zeigt die häufigsten Angriffe über das Netzwerk.
- **Häufigste Quellen für Angriffe über das Netzwerk**
  Zeigt die häufigsten Quellen für Angriffe über das Netzwerk.
- **Verlauf der Angriffe über das Netzwerk**
  Zeigt den Verlauf von Angriffen über das Netzwerk.
- **Kombinierter Bericht: Clients mit den meisten Angriffen über das Netzwerk / Häufigste Angriffe über das Netzwerk**
  Zeigt die Clients mit den meisten Angriffen über das Netzwerk sowie (durch Klicken auf den jeweiligen Clientnamen) die häufigsten Angriffe für jeden dieser Clients.
- **Clients mit den meisten Spam-SMS**
  Zeigt die Clients mit den meisten Spam-SMS.
- **Größte SMS-Spammer**
  Zeigt die größten SMS-Spammer für die ausgewählten Zielobjekte.
- **SMS-Spam - Verlauf**
  Zeigt den Verlauf von SMS-Spam.
- **Kombinierter Bericht: Clients mit den meisten Spam-SMS / Größte SMS-Spammer**
  Zeigt die Clients mit den meisten Spam-SMS sowie (durch Klicken auf den jeweiligen Clientnamen) die größten SMS-Spammer für jeden dieser Clients.

- **Clientbericht**, **Bedrohungsbericht**, **Firewall-Bericht**, **Ereignisbericht**, **Scanbericht**, **Taskbericht**, **Mobilgeräte-Bericht**, **Quarantänebericht**
  Grundlegende Berichte mit den Informationen, die Sie auch auf den Registerkarten Clients, Bedrohungs-Log, Ereignis-Log, Scan-Log bzw. Tasks finden.
- **Sammelbericht - Bedrohungen**
  Zusammenfassung aus den Berichten „Kombinierter Bericht: Clients mit den meisten Bedrohungen / Häufigste Bedrohungen", „Kombinierter Bericht: Häufigste Bedrohungen / Verlauf der Bedrohungen im Vergleich" sowie „Verlauf der Bedrohungen".
- **Sammelbericht - Angriffe über das Netzwerk**
  Zusammenfassung aus den Berichten „Kombinierter Bericht: Clients mit den meisten Angriffen über das Netzwerk / Häufigste Angriffe über das Netzwerk", „Häufigste Angriffe über das Netzwerk", „Häufigste Quellen für Angriffe über das Netzwerk" sowie „Verlauf der Angriffe über das Netzwerk".
- **Sammelbericht - SMS-Spam**
  Zusammenfassung aus den Berichten „Kombinierter Bericht: Clients mit den meisten Spam-SMS / Größte SMS-Spammer", „Größte SMS-Spammer" sowie „SMS-Spam - Verlauf"

Im Bereich **Filter** können Sie über die Listen **Clients** und **Bedrohung** auswählen, welche Clients und Bedrohungen in den Bericht einbezogen werden sollen.

Über die Schaltfläche **Weitere Einstellungen** können Sie zusätzliche Details festlegen. Hauptsächlich beziehen sich diese auf die Daten im Berichtkopf sowie die Art der verwendeten Diagramme. Sie können hier jedoch auch die Daten nach dem Status ausgewählter Attribute filtern und festlegen, welches Berichtformat verwendet wird (.html, .csv).

Auf der Registerkarte „Zeitraum" legen Sie fest, für welchen Zeitraum der Bericht erstellt wird:

- **Laufender Zeitraum**
  Bewirkt, dass der Bericht nur die Ereignisse enthält, die im ausgewählten laufenden Zeitraum aufgetreten sind. Wenn Sie zum Beispiel am Mittwoch einen Bericht für die laufende Woche erstellen, enthält er die Ereignisse von Sonntag (Wochenanfang) bis Mittwoch.

- **Abgeschlossener Zeitraum**
  Bewirkt, dass der Bericht nur die Ereignisse enthält, die im ausgewählten abgeschlossenen Zeitraum aufgetreten sind (z. B. im gesamten August oder in einer vollen Woche vom Sonntag bis zum folgenden Samstag). Wenn Sie die Option **Auch laufenden Zeitraum einbeziehen** aktivieren, enthält der Bericht außerdem auch die Ereignisse zwischen dem Abschluss des betreffenden Zeitraums und der Erstellung des Berichts.

Beispiel:

Nehmen wir an, Sie möchten einen Bericht mit den Ereignissen der vergangenen Kalenderwoche (von Sonntag bis Samstag) erstellen. Der Bericht soll am Mittwoch der darauffolgenden Woche erstellt werden.

Wählen Sie auf der Registerkarte **Zeitraum** die Option **Abgeschlossener Zeitraum** und geben Sie **1 Wochen** an. Deaktivieren Sie das Kontrollkästchen **Auch laufenden Zeitraum einbeziehen**. Setzen Sie auf der Registerkarte **Taskplaner** das **Intervall** auf **Woche** und wählen Sie **Mittwoch**. Die restlichen Einstellungen können Sie je nach Bedarf einrichten.

- **Von / Bis**
  Verwenden Sie diese Einstellung, um einen exakten Berichtszeitraum festzulegen.

Auf der Registerkarte **Taskplaner** können Sie im Bereich **Intervall** einrichten, dass der Bericht automatisch zu einem bestimmten Zeitpunkt oder in einem festgelegten Intervall ausgeführt wird.

Nachdem Sie den Ausführungszeitpunkt eingerichtet haben, klicken Sie auf **Ziel auswählen**, um festzulegen, wo der Bericht gespeichert werden soll. Berichte können in ERAS gespeichert (Standardeinstellung), per E-Mail an eine bestimmte Adresse geschickt oder in einen Ordner exportiert werden. Die letzte Option eignet sich beispielsweise, um einen Bericht auf einer Freigabe im Intranet zu speichern, um ihn auch anderen Mitarbeitern zugänglich zu machen.

Für den E-Mail-Versand von Berichten müssen Sie zunächst den SMTP-Server und die Absenderadresse einrichten (über **Extras** > **Serveroptionen** > **Sonstige Einstellungen**).

Um die aktuell definierten Berichteinstellungen als Template zu speichern, klicken Sie auf **Speichern** oder **Speichern unter**. Wenn Sie eine neue Template erstellen, klicken Sie auf **Speichern unter** und geben ihr einen passenden Namen.

Im oberen Teil des Konsolenfensters sehen Sie im Bereich **Bericht-Templates** die Namen der bereits erstellten

Templates. Zu jeder Template ist der Ausführungszeitpunkt/-turnus sowie die letzte Ausführung vermerkt. Unabhängig vom festgelegten Intervall können Sie einen Bericht jederzeit auf Abruf erstellen, indem Sie auf der Registerkarte **Optionen** auf **Jetzt erstellen** klicken.

Um eine vorhandene Bericht-Template als *.xml*-Datei zu importieren/exportieren, klicken Sie auf **Importieren/ Exportieren**. Wenn beim Import ein Namenskonflikt auftritt (d. h. die zu importierende Template hat denselben Namen wie eine bereits vorhandene Template), wird dieser gelöst, indem an den Namen der importierten Template eine zufällig gewählte Zeichenfolge angehängt wird.

Bereits erstellte Berichte können Sie über die Registerkarte **Erstellte Berichte** anzeigen. Für weitere Optionen wählen Sie einen oder mehrere Berichte aus und drücken die rechte Maustaste, um das Kontextmenü zu öffnen.

Wenn Sie eine Template in die Liste **Favoriten** aufnehmen, können Sie später schnell darauf zugreifen, um einen neuen Bericht zu erzeugen. Um eine Template in die Favoritenliste aufzunehmen, klicken Sie mit der rechten Maustaste auf den Bericht und wählen im Kontextmenü **Zu Favoriten hinzufügen**.

7.1 Beispielszenario für die Berichtfunktionen

Um ein durchgängig hohes Sicherheitsniveau auf Ihren Clients zu gewährleisten, brauchen Sie einen guten Überblick über den Sicherheitsstatus in Ihrem Netzwerk. Hierzu können Sie komfortabel und unkompliziert Berichte mit ausführlichen Informationen zu Bedrohungen, Updates, Client-Produktversionen usw. erstellen (nähere Informationen siehe Abschnitt Berichte 76). In der Regel liefert Ihnen ein wöchentlicher Bericht alle nötigen Informationen. In manchen Situationen ist jedoch eventuell erhöhte Wachsamkeit gefordert, etwa nachdem eine Bedrohung erkannt wurde.

Um die Berichtfunktionen an einem Beispiel zu illustrieren, werden wir eine parametrische Gruppe namens *Quarantäne* erstellen. Diese Gruppe soll nur Computer enthalten, auf denen beim letzten On-Demand-Scan eine Bedrohung erkannt und entfernt wurde. Definieren Sie diese Bedingung, indem Sie die Option **HAT Bedrohung bei letztem Scan gefunden** aktivieren. Zum Erstellen dieser parametrischen Gruppe gehen Sie wie im Abschnitt Parametrische Gruppen 54 beschrieben vor.

HINWEIS: Achten Sie beim Erstellen der Gruppe *Quarantäne* darauf, dass die Option **Permanent** deaktiviert bleibt. So werden die Computer der Gruppe dynamisch zugewiesen und wieder entfernt, sobald die Bedingung nicht mehr erfüllt ist.

Erstellen Sie den Bericht *Quarantäne-Computer*. Hierzu gehen Sie wie im Abschnitt Berichte 76 beschrieben vor. Verwenden Sie für unser Beispiel die folgenden Einstellungen:

- Einstellungen auf der Registerkarte **Optionen**:

Typ: **Quarantänebericht mit Details**
Stil: **Blue Scheme**
Clients: **Nur ausgewählte Gruppen**
Bedrohung: **entfällt**

- Einstellungen auf der Registerkarte **Zeitraum**:

Laufender Zeitraum: **Tag**

- Einstellungen auf der Registerkarte **Taskplaner**:

Intervall: **Tage**
Alle: **1 Tage**

TIPP: Sie können die Ergebnisse in der Berichtdatenbank speichern oder einen Ordner festlegen, in dem die fertigen Berichte abgelegt werden sollen. Außerdem können die Berichte per E-Mail verschickt werden. All diese Einstellungen stehen Ihnen über die Schaltfläche **Ziel auswählen** zur Verfügung.

Die erstellten Berichte können Sie auf der Registerkarte **Erstellte Berichte** einsehen.

Zusammenfassung: Wir haben die parametrische Gruppe *Quarantäne* erstellt, die alle Computer enthält, bei denen im letzten On-Demand-Scan eine Bedrohung erkannt wurde. Als nächstes haben wir einen regelmäßig ausgeführten Bericht erstellt, der uns jeden Tag darüber informiert, welche Computer der Gruppe *Quarantäne* angehören. So erhalten wir einen guten Überblick über den Status unserer Clients und können mögliche Bedrohungen unter Kontrolle halten.

TIPP: Um ausführliche Log-Informationen zu den letzten Scans zu erhalten, können Sie den Bericht **Scanbericht mit Details** verwenden.

8. Konfiguration von ESET Remote Administrator Server (ERAS)

8.1 Sicherheit

ESET Security-Lösungen ab der Version 3.x (ESET Smart Security usw.) bieten einen Passwortschutz für die unverschlüsselte Kommunikation zwischen dem Client und ERAS (Kommunikation per TCP, Port 2222).

Frühere Versionen (2.x) bieten diese Möglichkeit nicht. Falls eine Rückwärtskompatibilität mit früheren Versionen erforderlich ist, muss die Option **Zugriff ohne Authentifizierung für Clients erlauben** aktiviert werden.

Über die Optionen auf der Registerkarte „Sicherheit" lässt sich ein gleichzeitiger Betrieb von Security-Lösungen der Versionen 2.x und 3.x in einem Netzwerk ermöglichen.

- **Passwort für Konsole (Administratorzugriff, Read-Only-Zugriff)**
  Hier können Sie ein Passwort für den Administrator und für Benutzer mit Read-Only-Zugriff (Lesezugriff) festlegen, um die ERAC-Einstellungen vor unbefugten Änderungen zu schützen.

- **Passwort für Clients (ESET Security-Produkte)**
  Legt das Passwort fest, das Clients für den Verbindungsaufbau zum ERAS benötigen.

- **Passwort für Replikation**
  Legt das Passwort fest, das untergeordnete ERA Server für die Replikation von Daten auf den aktuellen ERAS benötigen.

- **Passwort für ESET Remote Installer (Agent)**
  Legt das Passwort fest, das der Installer-Agent für eine Verbindung zum ERAS benötigt. Relevant für Remoteinstallationen.

- **Zugriff ohne Authentifizierung für Clients erlauben (ESET Security-Produkte)**
  Wenn diese Option aktiviert ist, können auch Clients ohne gültiges Passwort (d. h. aktuelles Passwort weicht vom eingestellten „Passwort für Clients" ab) eine Verbindung zum ERAS aufbauen.

- **Zugriff ohne Authentifizierung für Replikation erlauben**
  Wenn diese Option aktiviert ist, können auch Clients von untergeordneten ERA Servern ohne gültiges Passwort für die Replikation eine Verbindung zum ERAS aufbauen.

- **Zugriff ohne Authentifizierung für ESET Remote Installer (Agent) erlauben**
  Wenn diese Option aktiviert ist, kann der ESET Remote Installer auch ohne gültiges Passwort auf ERAS zugreifen.

HINWEIS: Wenn die Authentifizierung sowohl in ERAS als auch auf allen Clients (Version 3.x oder höher) aktiviert ist, kann die Option **Zugriff ohne Authentifizierung für Clients erlauben** deaktiviert werden.

- **Windows-/Domänen-Authentifizierung verwenden**
  Aktiviert die Windows-/Domänen-Authentifizierung. Sie können festlegen, welche Gruppen Administratorzugriff (Vollzugriff auf ERA Server) und welche Gruppen nur Read-Only-Zugriff haben sollen (Option **Allen anderen Benutzern nur Read-Only-Zugriff geben**).

8.2 Serverwartung

Bei korrekter Konfiguration auf der Registerkarte „Serverwartung" wird die Datenbank von ERAS automatisch und ohne weiteren Konfigurationsbedarf gewartet und optimiert. Standardmäßig werden Einträge und Logs gelöscht, sobald sie älter als sechs Monate sind. Alle 15 Tage findet außerdem eine regelmäßige Komprimierung/Reparatur statt. Um die Optionen für die Serverwartung einzurichten, verwenden Sie den Menüpunkt **Extras** > **Serveroptionen** > **Serverwartung**.

Es stehen die folgenden Optionen zur Verfügung:

- **Clients löschen, wenn keine Verbindung in den letzten X Monaten/Tagen**
  Bewirkt, dass Clients, die im angegebenen Zeitraum (festgelegte Anzahl von Monaten/Tagen) keine Verbindung zu ERAS aufgebaut haben, automatisch gelöscht werden.

- **Bedrohungs-Logs löschen, wenn älter als X Monate/Tage**
  Bewirkt, dass Bedrohungs-Logs gelöscht werden, sobald sie älter als die angegebene Anzahl von Monaten (oder Tagen) sind.

- **Firewall-Logs löschen, wenn älter als X Monate/Tage**
  Bewirkt, dass Firewall-Logs gelöscht werden, sobald sie älter als die angegebene Anzahl von Monaten (oder Tagen) sind.

- **Ereignis-Logs löschen, wenn älter als X Monate/Tage**
  Bewirkt, dass Systemereignisse gelöscht werden, sobald sie älter als die angegebene Anzahl von Monaten (oder Tagen) sind.

- **Scan-Logs löschen, wenn älter als X Monate/Tage**
  Bewirkt, dass Scan-Logs gelöscht werden, sobald sie älter als die angegebene Anzahl von Monaten (oder Tagen) sind.

- **Mobilgeräte-Logs löschen, wenn älter als X Monate/Tage**
  Bewirkt, dass Mobilgeräte-Logs gelöscht werden, sobald sie älter als die angegebene Anzahl von Monaten (oder Tagen) sind.

- **Quarantäneeinträge ohne Clients löschen, wenn älter als X Monate/Tage**
  Bewirkt, dass Scan-Logs gelöscht werden, sobald sie älter als die angegebene Anzahl von Monaten (oder Tagen) sind.

Intervall für die Bereinigung
Legt fest, in welchem Intervall die oben festgelegten Löschaktionen durchgeführt werden.

Intervall für Komprimierung/Reparatur
Bewirkt, dass die Datenbank im angegebenen Intervall und zur festgelegten Uhrzeit komprimiert wird. Ein solcher Komprimierungs-/Reparaturlauf behebt Inkonsistenzen und Fehler und beschleunigt den Zugriff auf die Datenbank.

8.3 Mirror-Server

Mit der Mirror-Funktion können Sie einen lokalen Update-Server einrichten. Clientcomputer laden Updates für die Signaturdatenbank dann nicht von ESETs Internet-Servern, sondern vom Mirror-Server im lokalen Netzwerk herunter. Hauptvorteil einer solchen Lösung ist, dass sie sowohl das über die Internetverbindung übertragene Datenvolumen als auch die Anzahl der abgehenden Verbindungen deutlich reduziert. Statt Hunderten von Clientrechnern muss nur noch der Mirror-Server die Updates aus dem Internet herunterladen. Allerdings ist bei einer solchen Konfiguration zu beachten, dass der Mirror-Server eine ständige Internetverbindung haben muss.

Warnung: Wenn auf einem Mirror-Server ein Programmkomponenten-Upgrade (PCU) ohne anschließenden Neustart durchgeführt wird, kann dies zu Ausfällen führen. In einer solchen Situation kann der Server keine Updates mehr herunterladen oder für die Clientrechner bereitstellen. AKTIVIEREN SIE DAHER UNTER KEINEN UMSTÄNDEN AUTOMATISCHE PROGRAMMKOMPONENTEN-UPGRADES FÜR ESET SERVERPRODUKTE! Dieser Hinweis gilt nicht für Mirrors, die in ERAS erstellt wurden.

Die Mirror-Funktion steht an zwei Stellen zur Verfügung:

- ESET Remote Administrator (Mirror wird intern in ERAS ausgeführt und kann über ERAC verwaltet werden)

- ESET Smart Security Business Edition oder ESET NOD32 Antivirus Business Edition (sofern die Business Edition mit einem entsprechenden Lizenzschlüssel aktiviert wurde)

Die Methode zum Aktivieren der Mirror-Funktion wird vom Administrator ausgewählt.

In großen Netzwerken können mehrere Mirror-Server (z. B. für unterschiedliche Abteilungen eines Unternehmens) in Kombination mit einem zentralen Mirror-Server in einer mehrstufigen Hierarchie eingerichtet werden - ähnlich wie bei einer ERAS-Konfiguration mit mehreren Clients.

Um die Mirror-Funktion in ERAS zu aktivieren, müssen Sie als Administrator den Lizenzschlüssel für das erworbene Produkt sowie den Benutzernamen mit Passwort eingeben. Wenn Sie zunächst einen Lizenzschlüssel, einen Benutzernamen und ein Passwort für ESET NOD32 Antivirus Business Edition verwenden und später auf ESET Smart Security Business Edition upgraden, müssen Sie dementsprechend den ursprünglichen Lizenzschlüssel samt Benutzernamen und Passwort ersetzen.

HINWEIS: Updates für Clients mit ESET NOD32 Antivirus können auch über eine Lizenz für ESET Smart Security bezogen werden. Der umgekehrte Weg ist jedoch nicht möglich.

8.3.1 Betrieb des Mirror-Servers

Der Computer mit dem Mirror-Server sollte ständig eingeschaltet sein und über eine Verbindung zum Internet bzw. zu einem übergeordneten Mirror-Server (zur Replikation) verfügen. Die Update-Pakete für den Mirror-Server können auf zwei verschiedene Weisen heruntergeladen werden:

1. Per HTTP-Protokoll (empfohlen)
2. Über eine Netzwerkfreigabe (SMB)

Die ESET-Update-Server verwenden das HTTP-Protokoll mit Authentifizierung. Auf einem zentralen Mirror-Server sollte daher zum Zugriff auf die Update-Server der korrekte Benutzername (in der Regel im Format *EAV-XXXXXXX*) samt Passwort eingerichtet werden.

Der integrierte Mirror-Server von ESET Smart Security/ESET NOD32 Antivirus verfügt über einen integrierten HTTP-Server (Variante 1).

HINWEIS: Wenn Sie den integrierten HTTP-Server (ohne Authentifizierung) verwenden, stellen Sie bitte sicher, dass kein Zugriff von außerhalb ihres Netzwerks (d. h. durch Clients, die nicht durch Ihre Lizenz abgedeckt sind) möglich ist. Es darf kein Zugriff auf den Server über das Internet möglich sein.

Standardmäßig nimmt der integrierte HTTP-Server Verbindungen über den TCP-Port 2221 entgegen. Bitte stellen Sie sicher, dass dieser Port von keiner anderen Anwendung verwendet wird.

HINWEIS: Bei der Bereitstellung von Updates über den integrierten HTTP-Server wird ein Höchstwert von 400 Clients pro Update-Mirror empfohlen. In großen Netzwerken mit mehr Clients sollten die Mirror-Updates auf mehrere Mirror-Server (ERA oder ESS/EAV) verteilt werden. Falls zwingend ein einziger zentraler Mirror-Server verwendet werden muss, empfiehlt sich der Einsatz eines anderen HTTP-Servers wie z. B. Apache. ERA unterstützt dann auch andere Authentifizierungsverfahren (bei Apache wird z. B. die Methode über die .htaccess-Datei verwendet).

Bei der zweiten Methode (Netzwerkfreigabe) muss der Ordner mit den Update-Paketen für den Lesezugriff freigegeben werden. Auf den Client-Arbeitsplatzrechnern ist dementsprechend der Benutzername und das Passwort eines Benutzers mit Leserechten für den Update-Ordner einzutragen.

HINWEIS: ESET Clientlösungen verwenden das Benutzerkonto SYSTEM und haben daher andere Netzwerkzugriffsrechte als der aktuell angemeldete Benutzer. Es ist also auch dann eine separate Authentifizierung erforderlich, wenn das Netzlaufwerk für die Gruppe „Jeder" freigegeben ist und auch der aktuell angemeldete Benutzer darauf zugreifen kann. Achten Sie außerdem bitte darauf, dass Sie den Netzwerkpfad zu dem lokalen Server als UNC-Pfad angeben. Pfadangaben im Format *LAUFWERK:* werden nicht empfohlen.

Bei der Verwendung einer Netzwerkfreigabe (Variante 2) empfiehlt es sich, für den Zugriff einen eigenen Benutzer zu erstellen (z. B. NODUSER). Dieses Konto verwenden Sie dann auf allen Clientrechnern einzig dazu, um Updates herunterzuladen. Hierzu benötigt das Konto (in unserem Beispiel NODUSER) natürlich Leserechte für die Netzwerkfreigabe mit den Update-Paketen.
Geben Sie den Benutzernamen bei der Anmeldung an einem Netzlaufwerk bitte qualifiziert an, also im Format *ARBEITSGRUPPE\Benutzer* bzw. *DOMÄNE\Benutzer*.

Neben den Anmeldedaten müssen Sie auch die Quelle der Updates für die ESET Clientlösungen festlegen. Hierbei handelt es sich entweder um die URL-Adresse eines lokalen Servers (*http://Mirrorservername:Port*) oder den UNC-Pfad eines Netzlaufwerks: (*\\Mirrorservername\Freigabename*).

8.3.2 Update-Typen

Neben Updates für die Signaturdatenbank (die gleichzeitig auch Updates für den ESET Software-Kernel enthalten können) gibt es eine weitere Art von Updates: so genannte Programmkomponenten-Upgrades. Programmkomponenten-Upgrades erweitern ein Security-Produkt um neue Funktionen. Nach ihrer Installation ist ein Neustart erforderlich.

In den Einstellungen für den Mirror-Server können Sie als Administrator verhindern, dass Programm-Upgrades automatisch von den Update-Servern oder einem übergeordneten Mirror-Server heruntergeladen und an die Clients weitergegeben werden. So können Sie zunächst überprüfen, ob ein neues Update eventuell Konflikte mit vorhandenen Anwendungen verursacht. Wenn alles in Ordnung ist, können Sie die Weitergabe des Updates an die Clients anschließend manuell anstoßen.

Dies ist besonders dann praktisch, wenn Sie Updates für die Signaturdatenbank herunterladen und verwenden möchten, gleichzeitig aber auch eine neue Programmversion verfügbar ist. In Verbindung mit der aktuellen Signaturdatenbank-Version bietet auch die ältere Programmversion weiterhin optimalen Schutz. Dennoch empfiehlt es sich generell, die jeweils neueste Softwareversion herunterzuladen und zu installieren, um alle aktuellen Programmfunktionen nutzen zu können.

Standardmäßig werden Programmkomponenten nicht automatisch heruntergeladen. Wenn Sie einen automatischen Download wünschen, müssen Sie dies von Hand in ERAS konfigurieren. Nähere Informationen finden Sie im Kapitel Aktivieren und Konfigurieren des Update-Mirrors 82.

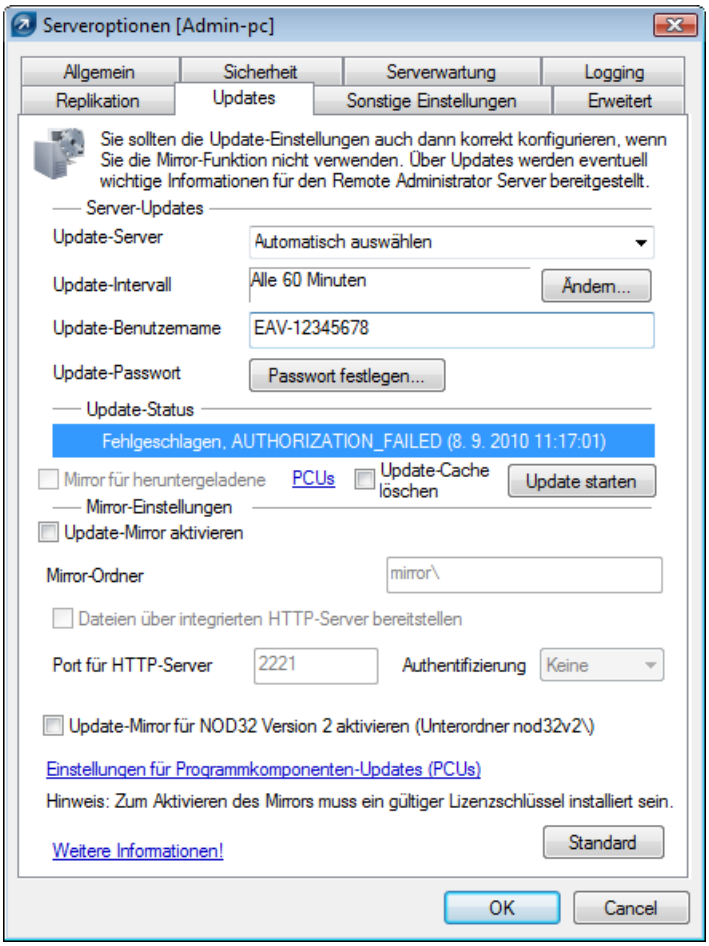
8.3.3 Aktivieren und Konfigurieren des Mirror-Servers

Wenn der Mirror-Server direkt in ERA integriert ist (Business Edition-Komponente), bauen Sie in ERAC eine Verbindung zu ERAS auf und führen dann die folgenden Schritte durch:

- Klicken Sie in ERAC auf **Extras** > **Serveroptionen** > **Updates**.
- Wählen Sie in der Liste **Update-Server** die Option **Automatisch auswählen** (Updates werden von den ESET-Servern heruntergeladen) oder geben Sie die URL bzw. den UNC-Pfad eines Mirror-Servers ein.
- Stellen Sie das Update-Intervall ein (Empfehlung: 60 Minuten).
- Wenn Sie im vorherigen Schritt **Automatisch auswählen** ausgewählt haben, geben Sie in den Feldern **Update-Benutzername** und **Update-Passwort** den Benutzernamen und das Passwort ein, die Sie beim Kauf erhalten haben. Falls Sie auf einen anderen Server im Netzwerk zugreifen, geben Sie einen gültigen Domänenbenutzer samt Passwort für diesen Server an.
- Aktivieren Sie die Option **Update-Mirror aktivieren** und geben Sie den Pfad zu dem Ordner ein, in dem die Update-Dateien gespeichert werden sollen. Standardmäßig wird dieser Mirror-Ordner als relativer Pfad angegeben. Aktivieren Sie die Option **Dateien über integrierten HTTP-Server bereitstellen** und geben Sie im Feld **Port für HTTP-Server** den Port ein, den der HTTP-Server verwenden soll (standardmäßig 2221). Setzen Sie die Einstellung **Authentifizierung** auf **Keine** (nähere Informationen siehe Kapitel Betrieb des Mirror-Servers 81).

HINWEIS: Falls Probleme bei den Updates auftreten, aktivieren Sie die Option **Update-Cache löschen**, um den Ordner mit den temporären Update-Dateien zu leeren.

- Über die Option **Mirror für heruntergeladene PCUs** können Sie die Mirror-Funktion für Programmkomponenten aktivieren. Zum Einrichten des PCU-Mirrors klicken Sie auf **Erweitert > Erweiterte Einstellungen bearbeiten** und konfigurieren die Einstellungen unter **ESET Remote Administrator** > **ERA Server** > **Einstellungen > Update-Mirror** (bzw. **Mirror für NOD32 Version 2**).
- Wählen Sie aus, welche Sprachversionen heruntergeladen werden sollen (**Erweitert** > **Erweiterte Einstellungen bearbeiten**, Zweig **ERA Server** > **Einstellungen** > **Update-Mirror** > **Mirror-Kopie der ausgewählten Programmkomponenten erstellen**. Sie sollten die Komponenten für alle Sprachversionen auswählen, die im Netzwerk verwendet werden sollen. Nicht benötigte Sprachversionen sollten Sie hingegen nicht herunterladen, um keinen unnötigen Datenverkehr im Netzwerk zu verursachen.



Die Mirror-Funktion steht auch direkt über die Programmoberfläche in ESET Smart Security Business Edition und ESET NOD32 Antivirus Business Edition zur Verfügung. Auf welche Weise Sie den Mirror-Server implementieren, bleibt Ihnen als Administrator überlassen.

Um den Mirror-Server in ESET Smart Security Business Edition bzw. ESET NOD32 Antivirus Business Edition zu aktivieren und zu starten, gehen Sie wie folgt vor:

1) Installieren Sie ESET Smart Security Business Edition bzw. ESET NOD32 Antivirus Business Edition.

2) Öffnen Sie das Dialogfenster **Einstellungen** (F5) und klicken Sie auf **Allgemein** > **Lizenzen**. Klicken Sie auf **Hinzufügen**, wählen Sie die **.lic*-Datei aus und klicken Sie auf **Öffnen**. Nach der Installation der korrekten Lizenz können Sie nun die Mirror-Funktion konfigurieren.

3) Klicken Sie im Zweig **Update** auf **Konfigurieren** und dann auf die Registerkarte **Update-Mirror**.

4) Aktivieren Sie die Optionen **Update-Mirror aktivieren** sowie **Dateien über integrierten HTTP-Server bereitstellen**.

5) Geben Sie im Feld **Mirror-Ordner** den vollständigen Pfad zu dem Ordner ein, in dem die Update-Dateien gespeichert werden sollen.

6) Die Werte in den Feldern **Benutzername** und **Passwort** dienen als Anmeldedaten für Clients, die auf den Mirror-Ordner zugreifen wollen. In den meisten Fällen sind hier keine Einträge nötig.

7) Setzen Sie die Einstellung **Authentifizierung** auf **NONE**.

8) Legen Sie fest, welche Komponenten heruntergeladen werden sollen. Sie sollten die Komponenten für alle Sprachversionen auswählen, die im Netzwerk verwendet werden. Es werden nur die Komponenten angezeigt, die auf den ESET-Update-Servern zur Verfügung stehen.

HINWEIS: Um einen optimalen Betrieb zu gewährleisten, sollten Sie auch die Programmkomponenten herunterladen lassen und in den Mirror einbeziehen. Wenn diese Option deaktiviert ist, wird nur die Signaturdatenbank aktualisiert, nicht hingegen die Programmkomponenten. Wenn der integrierte Update-Mirror von ERA verwendet wird, können Sie diese Option in ERAC konfigurieren: **Extras** > **Serveroptionen** > Registerkarte **Erweitert** > **Erweiterte Einstellungen bearbeiten** > **ESET Remote Administrator** > **ERA Server** > **Einstellung** > **Update-Mirror**. Aktivieren Sie alle

Sprachversionen, die in Ihrem Netzwerk verwendet werden.

8.3.4 Update-Mirror für Clients mit NOD32 Version 2.x

In ESET Remote Administrator können Sie als Administrator auch Mirror-Kopien von Updates für Clientcomputer erstellen, auf denen ESET NOD32 Antivirus 2.x installiert ist. Hierzu aktivieren Sie die Option **Extras** > **Serveroptionen** > **Updates** > **Update-Mirror für NOD32 Version 2 aktivieren**. Diese Option steht nur in ERA zur Verfügung, nicht jedoch beim Update-Mirror der Business Edition der Clientlösungen (v3.x).

Wenn in Ihrem Netzwerk unterschiedliche Clientversionen (2.x/3.x) eingesetzt werden, sollten Sie den integrierten Update-Mirror von ERA verwenden. Wenn beide Update-Mirror auf dem gleichen Computer aktiviert werden (einer in ERAS für Clients der Version 2.x, der andere in einem Business Edition-Client für Clients der Version 3.x) und beide HTTP-Server denselben TCP-Port verwenden, kann es zu Konflikten kommen.

Die Updates für Clients der Version 2.x werden im Ordner „*nod32v2*" abgelegt. Hierbei handelt es sich um einen Unterordner des Mirror-Hauptordners. Die URL für den Zugriff lautet:

http://Mirrorservername:Port/nod32v2

Bei einem Netzlaufwerk lautet der UNC-Pfad:

\\Mirrorservername\Freigabename\nod32v2

ERA kann auch Programmkomponenten für Clients der Version 2.x herunterladen. Um festzulegen, für welche Programmkomponenten dies geschieht, klicken Sie auf **Extras** > **Serveroptionen** > Registerkarte **Erweitert** > **Erweiterte Einstellungen bearbeiten** und erweitern dann den Zweig **ESET Remote Administrator** > **ERA Server** > **Einstellungen** > **Mirror für NOD32 Version 2**. Um das Übertragungsvolumen zu reduzieren, sollten Sie nur die Sprachversionen auswählen, die in Ihrem Netzwerk tatsächlich eingesetzt werden.

8.4 Replikation

Eine Replikation kommt in größeren Netzwerken zum Einsatz, in denen mehrere ERA Server installiert sind (z. B. ein Unternehmen mit mehreren Standorten). Nähere Informationen finden Sie im Kapitel Installation 17.

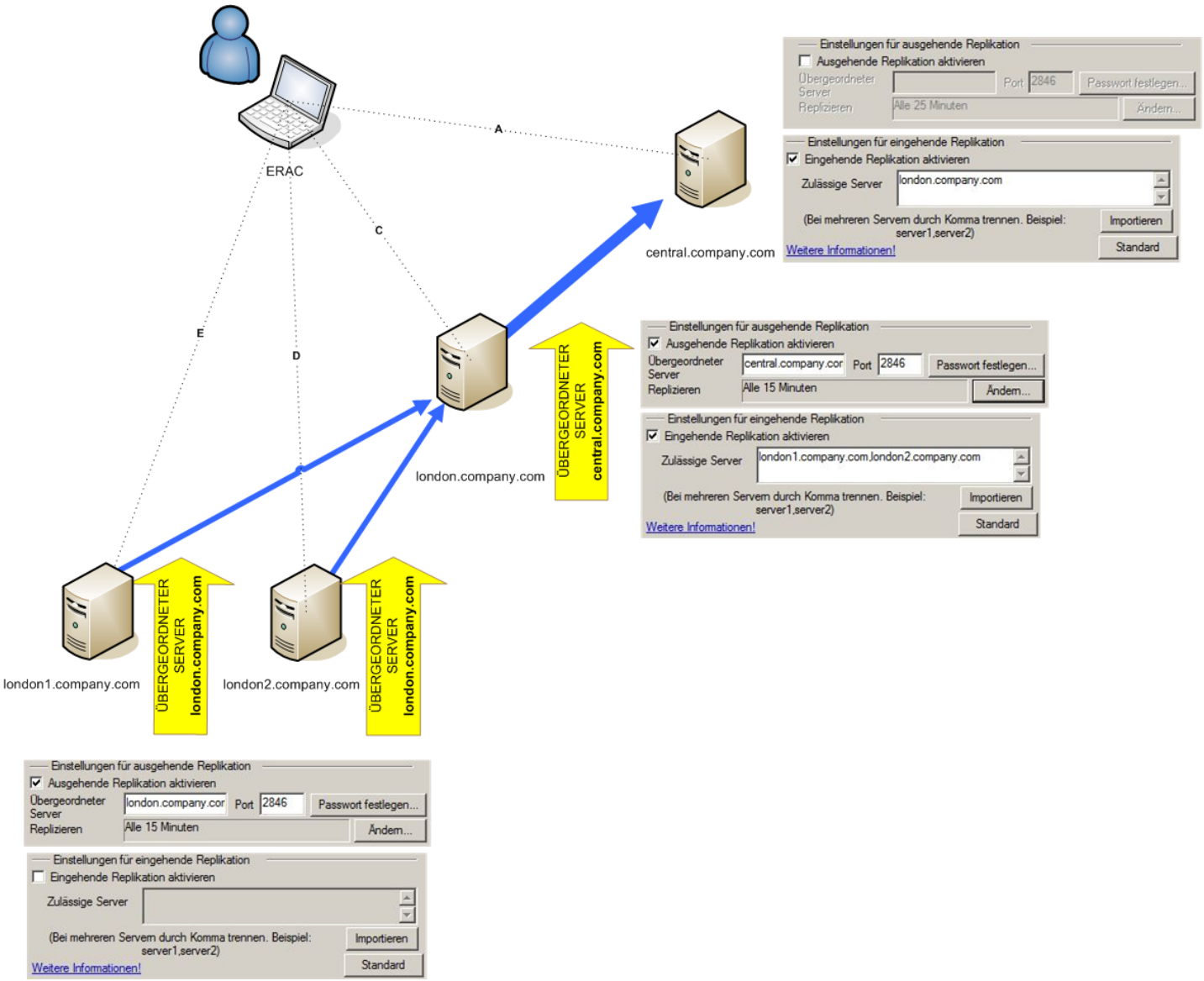
Die Optionen auf der Registerkarte **Replikation** (**Extras > Serveroptionen**) gliedern sich in zwei Bereiche:

- Einstellungen für ausgehende Replikation
- Einstellungen für eingehende Replikation

Zur Konfiguration von untergeordneten ERA Servern dienen die **Einstellungen für ausgehende Replikation**. Aktivieren Sie dazu die Option **Ausgehende Replikation aktivieren** und geben Sie die IP-Adresse oder den Hostnamen des Master-ERAS (übergeordneter Server) ein. Die Daten des untergeordneten Servers werden dann auf den Master-Server repliziert. Die **Einstellungen für eingehende Replikation** werden auf übergeordneten ERA Servern (Master-Servern) konfiguriert, damit diese die Daten der untergeordneten ERA Server entgegennehmen bzw. an andere übergeordnete Master-Server weiterleiten. Aktivieren Sie dazu die Option **Eingehende Replikation aktivieren** und legen Sie die Namen der zulässigen untergeordneten Server fest (bei mehreren Servern jeweils durch ein Komma getrennt).

Auf einem ERA Server in der Mitte einer Replikationshierarchie, für den es sowohl übergeordnete als auch untergeordnete Server gibt, müssen beide Optionen aktiviert werden.

Die unten stehende Abbildung zeigt alle der vorgenannten Szenarien. Jeder beige Computer steht für einen ERA Server. Für jeden ERAS sind der Name (zur besseren Übersicht identisch mit dem *Computernamen*) sowie die entsprechenden Einstellungen im Replikations-Dialogfenster angegeben.



Das Replikationsverhalten der Server lässt sich mit den folgenden Optionen genauer festlegen:

- **Bedrohungs-Log replizieren**, **Firewall-Log replizieren**, **Ereignis-Log replizieren**, **Scan-Log replizieren**, **Mobilgeräte-Log replizieren**, **Quarantäne replizieren**
  Wenn diese Optionen aktiviert sind, werden alle Daten aus den einzelnen Spalten und Zeilen der Registerkarten **Clients**, **Bedrohungs-Log**, **Firewall-Log**, **Ereignis-Log**, **Scan-Log**, **Mobilgeräte-Log**, **Quarantäne** bzw. **Tasks** repliziert. Daten, die nicht direkt in der Datenbank, sondern in separaten Dateien gespeichert sind (*.txt*- oder *.xml*-Dateien), werden unter Umständen nicht repliziert. Aktivieren Sie diese Optionen, um auch Einträge in solchen Dateien zu replizieren.

- **Details zu Bedrohungs-Log automatisch replizieren**, **Details zu Scan-Log automatisch replizieren**, **Clientdetails automatisch replizieren**, **Details zu Mobilgeräte-Log automatisch replizieren**, **Quarantänedateien automatisch replizieren**
  Mit diesen Optionen wird die automatische Replikation von zusätzlichen Daten aktiviert, die in separaten Dateien gespeichert sind. Über die Schaltfläche **Anfordern** können Sie solche Daten auch je nach Bedarf herunterladen.

HINWEIS: Einige Logs werden automatisch repliziert, die dazugehörigen Details und Clientkonfigurationen jedoch nur auf Abruf. Grund dafür ist, dass einige Logs große Mengen von Daten enthalten, die oft nicht relevant sind. Ein Log eines Scans, bei dem die Option „Alle Dateien in Log aufnehmen" aktiv war, belegt beispielsweise recht viel Platz auf der Festplatte. Die Angaben zu den Dateien sind oft jedoch unnötig und können im Bedarfsfall problemlos von Hand angefordert werden. Beachten Sie außerdem, dass untergeordnete Server nicht automatisch melden, wenn ein Client gelöscht wird. Daten zu gelöschten Clients von untergeordneten Servern bleiben deshalb unter Umständen auf den übergeordneten Servern gespeichert. Damit gelöschte Clients in solch einem Fall automatisch von der Registerkarte „Clients" des übergeordneten Servers entfernt werden, aktivieren Sie die Option **Replizierte Clients löschen, wenn sie auf dem untergeordneten Server gelöscht werden** unter **Serveroptionen** > **Erweitert** > **Erweiterte Einstellungen bearbeiten** > **Einstellungen** > **Replikation**.

Um festzulegen, in welchem Umfang Logs in ERAS entgegengenommen werden, verwenden Sie die entsprechenden Optionen unter **Extras** > **Serveroptionen** > **Erweitert** > **Erweiterte Einstellungen bearbeiten** > **Einstellungen** > **Serverwartung**.

Wenn Sie nur Clients mit geändertem Status replizieren möchten, aktivieren Sie die Option **Extras** > **Serveroptionen** > **Replikation** > **Alle Clients für Replikation vormerken** neben der Schaltfläche **Replikation starten**.

8.5 Logging

Im laufenden Betrieb erstellt ERAS ein Log (**Log-Dateiname**) über die Serveraktivität. Den Umfang können Sie über die Option **Log-Umfang** anpassen. Wenn die Option **Logging in Textdatei** aktiviert ist, wird beim Erreichen einer bestimmten Größenschwelle (**Datei archivieren alle ... MB**) jeweils eine neue Log-Datei erstellt. Die archivierten Dateien werden nach einer bestimmten Anzahl von Tagen gelöscht (**Archivierte Logs löschen nach ... Tagen**).

Die Option **Logging in Anwendungs-Log des Betriebssystems** bewirkt, dass die Log-Daten in die Ereignisanzeige des Systems kopiert werden (**Windows-Systemsteuerung** > **Verwaltung** > **Ereignisanzeige**).

Die Option **Datenbank-Debug-Log** sollte unter normalen Umständen deaktiviert bleiben.

Die Textausgabe wird standardmäßig in der folgenden Datei gespeichert:
%ALLUSERSPROFILE%\Anwendungsdaten\Eset\ESET Remote Administrator\Server\logs\era.log

Die Einstellung „Log-Umfang" sollte in der Regel auf dem Standardwert „Stufe 2 - wie oben + wichtige Informationen zur Sitzung" belassen werden. Wählen Sie nur dann eine umfangreichere Logging-Stufe, wenn Probleme auftreten oder wenn Sie vom ESET-Support dazu aufgefordert werden.

Um die Komprimierungsstufe für die archivierten Logs einzurichten, klicken Sie auf **Extras** > **Serveroptionen** > **Erweitert** > **Erweiterte Einstellungen bearbeiten** > **Einstellungen** > **Logging** > **Komprimierung der archivierten Debug-Logs**.

8.6 Lizenzverwaltung

Für den ordnungsgemäßen Betrieb von ERA muss ein Lizenzschlüssel auf den Server übertragen werden. Wenn Sie einen Lizenzschlüssel erwerben, wird er Ihnen zusammen mit Ihrem Benutzernamen und Passwort per E-Mail zugeschickt. Zur Verwaltung der Lizenzen verwenden Sie den **Lizenz-Manager**.

ERA 3.x und höher unterstützt mehrere Lizenzschlüssel gleichzeitig. Dies erleichtert die Verwaltung der Lizenzschlüssel.

Das Hauptfenster des Lizenz-Managers öffnen Sie über den Menüpunkt **Extras** > **Lizenz-Manager**.

So fügen Sie einen neuen Lizenzschlüssel hinzu:

1) Klicken Sie auf **Extras** > **Lizenz-Manager** oder drücken Sie die Tastenkombination **Strg+L**.
2) Klicken Sie auf **Durchsuchen** und wählen Sie die gewünschte Lizenzschlüssel-Datei aus (die Dateien haben die Namenserweiterung *.lic*).
3) Klicken Sie zur Bestätigung auf **Öffnen**.
4) Überprüfen Sie die Angaben zum Lizenzschlüssel. Wenn sie richtig sind, wählen Sie **Auf Server übertragen**.
5) Klicken Sie zur Bestätigung auf **OK**.

Die Schaltfläche **Auf Server übertragen** ist nur aktiv, wenn Sie einen Lizenzschlüssel ausgewählt haben (über die Schaltfläche **Durchsuchen**). In diesem Bereich des Fensters werden auch Angaben zum aktuell ausgewählten Lizenzschlüssel angezeigt. So können Sie diese noch einmal überprüfen, bevor Sie den Schlüssel auf den Server kopieren.

Im mittleren Teil des Fensters sehen Sie Angaben zu dem Lizenzschlüssel, der aktuell vom Server verwendet wird. Um Informationen zu allen auf dem Server gespeicherten Lizenzschlüsseln anzuzeigen, klicken Sie auf **Details**.

ERAS kann jeweils den passendsten Lizenzschlüssel auswählen und mehrere Schlüssel zu einem einzigen zusammenführen. Wenn mehrere Lizenzschlüssel auf dem Server gespeichert sind, versucht ERAS stets, den Schlüssel mit den meisten Clients und der längsten noch verbleibenden Gültigkeitsdauer zu ermitteln.

Voraussetzung für das Zusammenführen mehrerer Schlüssel ist, dass alle Schlüssel auf denselben Kunden ausgestellt sind. Bei diesem unkomplizierten Vorgang wird ein neuer Schlüssel erstellt, der alle Clients aus den bisherigen

Schlüsseln umfasst. Als Ablaufdatum des neuen Lizenzschlüssels wird das früheste Ablaufdatum der bisherigen Lizenzschlüssel verwendet.

Im unteren Teil des Lizenz-Managers können Sie festlegen, ob bei Lizenzierungsproblemen eine Benachrichtigung erfolgen soll. Es stehen die folgenden Optionen zur Verfügung:

- **Warnen, wenn die Serverlizenz in 20 Tagen abläuft** - Bewirkt, dass x Tage vor dem Ablauf der Lizenz eine Warnung angezeigt wird.
- **Nur warnen, wenn dadurch die Anzahl der Clients in der Lizenz unter die Anzahl der vorhandenen Clients in der Serverdatenbank fallen würde** - Ist diese Option aktiviert, so wird die Warnung nur angezeigt, wenn durch den Ablauf des Lizenzschlüssels oder eines Teils der Lizenz die Anzahl der lizenzierten Clients unter die Anzahl der momentan verbundenen Clients, d. h. die Anzahl der Clients in der ERAS-Datenbank, fallen würde.
- **Warnen, wenn nur noch 10% freie Clients in der Serverlizenz verfügbar** - Bewirkt, dass der Server eine Warnung anzeigt, wenn der Anteil der noch für neue Clients verfügbaren Lizenzen unter den eingestellten Prozentwert fällt.

ERAS kann prinzipiell auch mehrere Lizenzen zusammenführen, die auf unterschiedliche Kunden ausgestellt sind. Diese Funktion muss jedoch durch einen speziellen Schlüssel freigeschaltet werden. Wenn Sie einen solchen Schlüssel benötigen, geben Sie dies bitte in Ihrer Bestellung an oder wenden Sie sich an Ihren zuständigen ESET-Vertriebspartner.

8.7 Erweiterte Einstellungen

Zum Zugriff auf die erweiterten Einstellungen für ERA klicken Sie auf **Extras** > **Serveroptionen** > **Erweitert** > **Erweiterte Einstellungen bearbeiten**.

Die erweiterten Einstellungen umfassen die folgenden Optionen:

- **Maximal ... Prozent der Festplatte belegen**
  Wenn dieser Wert überschritten wird, stehen bestimmte Serverfunktionen eventuell nicht mehr zur Verfügung. In diesem Fall wird beim Verbindungsaufbau zum ERAS eine Meldung in ERAC angezeigt.
- **Codierung für Kommunikationsprotokoll**
  Legt die Art der Codierung fest. Die Standardeinstellung wird empfohlen.
- **MAC-Adressangabe bei Bedarf ändern (unbekannt in gültig)**
  Diese Einstellung legt fest, was geschieht, wenn eine Clientsoftware, die eine Übermittlung der MAC-Adresse unterstützt (z. B. ein Client der Version 3.x), über eine Clientsoftware installiert wird, die dies nicht tut (z. B. ESET NOD32 Antivirus 2.x). Wenn sie aktiviert ist, wird der alte Clientdatensatz in diesem Fall in den neuen umgewandelt. Die Standardeinstellung (Ja) wird empfohlen.
- **MAC-Adressangabe bei Bedarf ändern (gültig in unbekannt)**
  Diese Einstellung legt fest, was geschieht, wenn eine Clientsoftware, die eine Übermittlung der MAC-Adresse nicht unterstützt (z. B. ein Client der Version 2.x), über eine Clientsoftware installiert wird, die dies tut (z. B. ESET NOD32 Antivirus 3.x). Wenn sie aktiviert ist, wird der alte Clientdatensatz in diesem Fall in den neuen umgewandelt. Die Standardeinstellung (Nein) wird empfohlen.
- **MAC-Adressangabe bei Bedarf ändern (gültig in gültig)**
  Aktiviert die Umbenennung gültiger MAC-Adressen. Mit dem Standardwert ist keine Umbenennung möglich, d. h. die MAC-Adresse ist Teil der eindeutigen Clientkennung. Deaktivieren Sie diese Option, wenn mehrere Einträge für denselben PC vorhanden sind. Außerdem sollten Sie diese Option deaktivieren, wenn ein Client nach einer Änderung der MAC-Adresse als derselbe Client erkannt wird.
- **Computernamen bei Bedarf ändern**
  Legt fest, ob Änderungen am Hostnamen von Clientcomputern zulässig sind. Wenn diese Einstellung deaktiviert ist, wird der Computername als Teil der eindeutigen Clientkennung verwendet.
- **Standard-Serveranmeldedaten auch bei Push-Installation verwenden**
  In ERAS können Sie einen Benutzernamen und ein Passwort ausschließlich für die Remoteinstallation per Anmeldeskript oder E-Mail festlegen. Aktivieren Sie diese Option, wenn die hinterlegten Anmeldedaten auch für die Push-Remoteinstallation verwendet werden sollen.

8.8 Sonstige Einstellungen

SMTP-Einstellungen
Für einige ERA-Funktionen ist eine korrekte SMTP-Serverkonfiguration erforderlich. Dies betrifft unter anderem die Remoteinstallation per E-Mail sowie den E-Mail-Versand von Berichten.

Neue Clients

Neue Clients zulassen
Wenn diese Option deaktiviert ist, werden keine neuen Clients auf die Registerkarte „Clients" aufgenommen. Selbst wenn ein Client eine Verbindung zu ERA Server aufbaut, erscheint er also nicht auf der Registerkarte „Clients".

Markierung „Neu" bei neuen Clients automatisch entfernen
Wenn diese Option aktiviert ist, wird die Markierung „Neu" bei Clients, die erstmals eine Verbindung zu ERAS aufbauen, automatisch entfernt. Nähere Informationen finden Sie im Kapitel Clients (Registerkarte) 25.

Ports
Hier können Sie einstellen, auf welchen Ports ERAS ankommende Verbindungen entgegennimmt. Dies erfolgt separat für Verbindungen von der **Konsole** (standardmäßig 2223), von einem **Client** (standardmäßig 2222), vom Replikationsprozess (**Replikationsport**, standardmäßig 2846) sowie vom **ESET Remote Installer** (standardmäßig 2224).

ThreatSense.Net
Wenn diese Option aktiviert ist, übermittelt ERAS verdächtige Dateien und statistische Informationen im festgelegten Zeitintervall von den Clients an die ESET-Server. Beachten Sie dabei, dass eine direkte Übermittlung dieser Daten von den Client-Arbeitsplatzrechnern aufgrund der Netzwerkkonfiguration nicht in jedem Fall möglich ist.

9. ESET Remote Administrator Maintenance Tool

Das ESET Remote Administrator Maintenance Tool dient zum Ausführen bestimmter Aufgaben rund um Betrieb und Wartung des Servers. Sie finden es unter **Start** > **Programme** > **ESET Remote Administrator** > **Server**. Nach dem Start des ERA Maintenance Tool führt Sie ein interaktiver Assistent durch die gewünschten Aufgaben.

HINWEIS: Zum korrekten Betrieb des ERA Maintenance Tool unter Windows NT4 SP6 ist Internet Explorer 5.0 oder höher erforderlich. Alternativ kann auch die Common-Controls-Bibliothek (comctl32.dll) aktualisiert werden. Die ComCtl32-Bibliothek ist Teil des Pakets „Platform SDK Comctl32 Redistributables", das Sie von der Microsoft-Website herunterladen können.

9.1 Angaben zum ERA Server

Das Tool zeigt zusammenfassende Informationen zum installierten ERA Server. Für ein separates Fenster mit ausführlicheren Angaben klicken Sie auf **Weitere Informationen**. Um die Informationen zu kopieren, klicken Sie auf **In Zwischenablage kopieren**, um sie zu aktualisieren, auf **Aktualisieren**. Nachdem Sie die Angaben überprüft haben, fahren Sie mit dem nächsten Schritt fort, indem Sie auf **Weiter** klicken.

9.2 Aufgabentyp

Das Maintenance Tool zeigt Ihnen eine Liste der verfügbaren Aufgaben. Nachdem Sie die Einstellungen für eine bestimmte Aufgabe festgelegt haben, können Sie diese Einstellungen speichern, indem Sie auf **Alle Einstellungen in Datei speichern** klicken. Später können Sie diese Einstellungen dann jederzeit wiederverwenden, indem Sie auf **Alle Einstellungen aus Datei laden** klicken. Die Aktionen **Alle Einstellungen in Datei speichern** und **Alle Einstellungen aus Datei laden** sind auch bei jedem Zwischenschritt verfügbar, während Sie die Einstellungen für die Aufgabe im Assistenten definieren.

9.2.1 ERA Server beenden

Diese Aufgabe beendet den ESET Remote Administrator Server-Dienst.

9.2.2 ERA Server starten

Diese Aufgabe startet den ESET Remote Administrator Server-Dienst.

9.2.3 Datenbank übertragen

Mit dieser Aufgabe können Sie das Datenbankformat umwandeln. Das Tool unterstützt eine Umwandlung zwischen den folgenden Datenbanktypen:

- MS Access
- MS SQL Server
- Oracle
- MySQL

Im ersten Schritt wählen Sie die Datenbank aus.

Bei einer MS Access-Datenbank geben Sie den Pfad zur *.mdb*-Datei an. Standardmäßig wird der bei der Installation von ERA Server angegebene Pfad verwendet.
Bei allen anderen Datenbanktypen müssen Sie eine Reihe zusätzlicher Parameter angeben:

- Verbindungsstring: Spezielle Zeichenfolge, die die Einstellungen für die Verbindung zur Quelldatenbank definiert
- Benutzername: Benutzername für den Zugriff auf die Datenbank
- Passwort: Passwort für den Zugriff auf die Datenbank
- Schemaname: Name eines Schemas (nur bei Oracle und MS SQL)

Klicken Sie auf **Aktuelle Serverkonfiguration laden**, um die aktuellen Einstellungen von ERA Server zu verwenden. Klicken Sie auf **Verbindung testen**, um die Datenbankverbindung zu testen. Falls keine Verbindung aufgebaut werden kann, überprüfen Sie die Parameter auf Fehler. Fahren Sie nach erfolgreichem Abschluss der Prüfung fort, indem Sie auf **Weiter** klicken.

Wählen Sie die Zieldatenbank aus. Wenn der Server nach erfolgreichem Abschluss der Umwandlung eine Verbindung zur neuen Datenbank aufbauen und diese zukünftig verwenden soll, aktivieren Sie die Option **Server-Verbindungseinstellungen** ersetzen. Wenn diese Option deaktiviert ist, wird zwar die neue Datenbank erstellt, der

Server verwendet diese jedoch im Anschluss nicht.

Bei allen Datenbanktypen außer MS Access wählen Sie im nächsten Schritt aus, ob die Datenbanktabellen automatisch erstellt werden sollen (**Automatisch Tabellen in der neuen Datenbank erstellen**) oder ob Sie sie später in die Datenbank einfügen möchten (**Skript anzeigen** > **In Datei speichern**). Bei einer MS SQL-Datenbank können Sie mit der Option **Automatisch neue Datenbank „ESETRADB" erstellen** automatisch eine neue MySQL-Datenbank namens ESETRADB erstellen lassen. Im letzten Schritt bestätigen Sie die Umwandlung der Datenbank.

9.2.4 Datenbank sichern

Das Tool bietet Ihnen die Möglichkeit, eine Sicherungskopie der Datenbank zu erstellen. Im ersten Fenster wählen Sie die Quelldatenbank aus. Die Einstellungen sind ähnlich wie beim Übertragen einer Datenbank (siehe Kapitel Datenbank übertragen 89). Im nächsten Schritt geben Sie an, in welche Sicherungsdatei die Quelldatenbank kopiert werden soll.

Mit den optionalen Parametern im unteren Teil des Fensters können Sie eine ggf. vorhandene Datei überschreiben (**Überschreiben, falls vorhanden**) sowie ESET Remote Administrator Server während der Sicherung beenden (**Server während Verarbeitung der Aufgabe beenden**). Klicken Sie auf **Weiter**, um den Vorgang zu starten.

9.2.5 Datenbank wiederherstellen

Das Tool bietet Ihnen die Möglichkeit, die Datenbank aus einer vorhandenen Sicherungskopie wiederherzustellen. Im ersten Fenster wählen Sie den Datenbanktyp aus. Die Einstellungen sind ähnlich wie beim Übertragen einer Datenbank (siehe Kapitel Datenbank übertragen 89).

Bei allen Datenbanktypen außer MS Access wählen Sie im nächsten Schritt aus, ob die Datenbanktabellen automatisch erstellt werden sollen (**Automatisch Tabellen in der neuen Datenbank erstellen**) oder ob Sie sie später in die Datenbank einfügen möchten (**Skript anzeigen** > **In Datei speichern**). Bei einer MS SQL-Datenbank können Sie mit der Option **Automatisch eine neue Datenbank (ESETRADB) erstellen** automatisch eine neue MySQL-Datenbank namens ESETRADB erstellen lassen. Im letzten Schritt bestätigen Sie die Umwandlung der Datenbank.

Im nächsten Schritt wählen Sie die Sicherungsdatei aus, aus der die Datenbank wiederhergestellt werden soll. Mit den optionalen Parametern im unteren Teil des Fensters können Sie auch Dateien aus einem anderen Datenbanktyp als im vorherigen Schritt ausgewählt importieren (**Import aus anderem Datenbanktyp zulassen**) sowie ESET Remote Administrator Server während der Wiederherstellung beenden (**Server während Verarbeitung der Aufgabe beenden**). Klicken Sie auf **Weiter**, um den Vorgang zu starten.

9.2.6 Tabellen löschen

Mit dieser Aufgabe werden die vorhandenen Datenbanktabellen gelöscht. Die Datenbank wird so wieder in den Zustand versetzt, den sie direkt nach der Installation von ERA Server hat. Im ersten Fenster wählen Sie den Datenbanktyp aus. Die Einstellungen sind ähnlich wie beim Übertragen einer Datenbank (siehe Kapitel Datenbank übertragen 89). Im nächsten Schritt werden Sie gebeten, die Aktion zu bestätigen. Wählen Sie **Zur Kenntnis genommen - Vorgang fortsetzen** und klicken Sie dann zur Bestätigung auf **Weiter**.

HINWEIS: Bei einer MS SQL-, MySQL- oder Oracle-Datenbank empfiehlt es sich, ERA Server vor dem Löschen der Tabellen zu beenden.
Wenn Sie mit einer MS Access-Datenbank arbeiten, wird diese durch die leere Standarddatenbank ersetzt.

9.2.7 Neuen Lizenzschlüssel installieren

Um einen neuen Lizenzschlüssel für den Server zu installieren, geben Sie seinen Speicherort an.
Falls erforderlich, können Sie den vorhandenen Lizenzschlüssel überschreiben (Option **Überschreiben, falls vorhanden**) sowie den Server neu starten (**Server starten, falls er nicht ausgeführt wird**). Klicken Sie auf **Weiter**, um den Vorgang zu starten.

9.2.8 Serverkonfiguration bearbeiten

Über diese Aufgabe können Sie den Configuration Editor starten (falls installiert). Nach Abschluss der Aufgabe wird der Configuration Editor geöffnet, wo Sie die erweiterten Einstellungen für ERA Server bearbeiten können. Dieselben Einstellungen finden Sie auch in der Konsole unter **Extras** > **Serveroptionen** > **Erweitert** > **Erweiterte Einstellungen bearbeiten**.

HINWEIS: Damit Sie diese Funktion nutzen können, muss ERA Console installiert sein.

10. Fehlerbehebung

10.1 Häufige Fragen (FAQ)

Dieses Kapitel enthält Antworten auf häufig gestellte Fragen sowie Problemlösungen rund um die Installation und Bedienung von ERA.

10.1.1 Probleme bei der Installation von ESET Remote Administrator auf Windows Server 2000/2003

Ursache:
Eventuell läuft der Terminalserver auf dem System im Ausführungsmodus (*execute*).

Lösung:
Microsoft empfiehlt, Systeme, auf denen der Terminalserver-Dienst aktiviert ist, während der Installation neuer Programme in den Installationsmodus (*install*) zu schalten. Dies können Sie entweder über den Punkt **Systemsteuerung** > **Software** oder durch Eingabe des Befehls *change user /install* in der Eingabeaufforderung bewirken. Nach der Installation geben Sie den Befehl *change user /execute* ein, um den Terminalserver wieder in den Ausführungsmodus zu schalten. Eine Schritt-für-Schritt-Anleitung zu diesem Vorgang finden Sie im folgenden Artikel: http://support.microsoft.com/kb/320185.

10.1.2 Was bedeutet der GLE-Fehlercode?

Bei der Installation von ESET Smart Security oder ESET NOD32 Antivirus über ESET Remote Administrator Console kann in seltenen Fällen ein GLE-Fehler auftreten. Um herauszufinden, wofür ein bestimmter GLE-Fehlercode steht, gehen Sie wie folgt vor:

1) Öffnen Sie eine Eingabeaufforderung. Klicken Sie hierzu zunächst auf **Start** > **Ausführen**. Geben Sie *cmd* ein und klicken Sie auf **OK**.
2) Geben Sie in der Eingabeaufforderung den folgenden Befehl ein: *net helpmsg Fehlercode*

Beispiel: *net helpmsg 55*

Ergebnis in diesem Beispiel: Die angegebene Netzwerkressource bzw. das angegebene Gerät ist nicht mehr verfügbar.

10.2 Gängige Fehlercodes

Im ERA-Betrieb können Fehlermeldungen mit Fehlercodes auftreten, die auf ein Problem mit einer bestimmten Funktion oder Aktion hinweisen. Die gängigsten Fehlercodes bei Push-Installationen sowie einige Fehlermeldungen aus dem ERAS-Log sind in den folgenden Kapiteln beschrieben.

10.2.1 Fehlermeldungen bei der Remoteinstallation von ESET Smart Security oder ESET NOD32 Antivirus über ESET Remote Administrator

SC-Fehlercode 6, GLE-Fehlercode 53: IPC-Verbindung zum Ziel-Computer konnte nicht hergestellt werden
Damit eine IPC-Verbindung hergestellt werden kann, müssen die folgenden Voraussetzungen gegeben sein:
1. Auf dem ERAS-Computer sowie dem Zielrechner muss der TCP/IP-Stack installiert sein.
2. Die Datei- und Druckerfreigabe für Microsoft-Netzwerke muss installiert sein.
3. Die Ports für die Dateifreigabe müssen geöffnet sein (135-139, 445).
4. Der Zielrechner muss auf ping-Anforderungen antworten.

SC-Fehlercode 6, GLE-Fehlercode 67: ESET Installer konnte nicht auf dem Ziel-Computer installiert werden
Die administrative Freigabe *ADMIN$* auf dem Systemlaufwerk des Clients muss zugänglich sein.

SC-Fehlercode 6, GLE-Fehlercode 1326: IPC-Verbindung zum Ziel-Computer konnte nicht hergestellt werden. Eventuell ist der Benutzername oder das Passwort falsch.
Benutzername und Passwort des Administratorkontos wurden nicht oder falsch eingegeben.

SC-Fehlercode 6, GLE-Fehlercode 1327: IPC-Verbindung zum Ziel-Computer konnte nicht hergestellt werden
Es wurde kein Administratorpasswort angegeben. Ohne Administratorpasswort kann jedoch keine Push-Remoteinstallation durchgeführt werden.

SC-Fehlercode 11, GLE-Fehlercode 5: ESET Installer konnte nicht auf dem Ziel-Computer installiert werden
Der Installer konnte wegen unzureichender Zugriffsrechte nicht auf den Clientcomputer zugreifen (Zugriff verweigert).

SC-Fehlercode 11, GLE-Fehlercode 1726: NOD32-Installer konnte nicht auf dem Ziel-Computer installiert werden
Dieser Fehlercode wird angezeigt, wenn bei wiederholten Installationsversuchen das Fenster für die Push-Installation nach dem ersten Versuch nicht geschlossen wurde.

10.2.2 Gängige Fehlercodes in era.log

0x1203 - UPD_RETVAL_BAD_URL
Fehler im Update-Modul - Name des Update-Servers wurde falsch eingegeben.

0x1204 - UPD_RETVAL_CANT_DOWNLOAD
Dieser Fehler kann in den folgenden Fällen auftreten:

- Bei einem Update über HTTP:
  - Der Update-Server gibt einen HTTP-Fehlercode im Bereich 400 bis 500 zurück (außer 401, 403, 404 und 407).
  - Updates werden von einem Server auf Cisco-Basis heruntergeladen, und das Format der HTML-Authentifizierungsantwort wurde geändert.

- Bei einem Update aus einem freigegebenen Ordner:
  - Der zurückgegebene Fehler passt nicht in die Kategorien „ungültige Authentifizierung" oder „Datei nicht gefunden" (z. B. *Verbindung unterbrochen*, *Server existiert nicht* usw.).

- Bei beiden Update-Methoden:
  - Es konnte keiner der Server aus der Datei *upd.ver* gefunden werden (Speicherort der Datei: *%ALLUSERSPROFILE%\Anwendungsdaten\ESET\ESET Remote Administrator\Server\updfiles*)
  - Es konnte keine Verbindung zum Failsafe-Server aufgebaut werden (vermutlich wurden die betreffenden ESET-Einträge in der Registrierung gelöscht).

- Bei einer falschen Proxyserver-Konfiguration in ERAS:
  - Der Proxyserver muss im korrekten Format angegeben werden.

0x2001 - UPD_RETVAL_AUTHORIZATION_FAILED
Authentifizierung am Update-Server ist fehlgeschlagen (Benutzername oder Passwort ist falsch).

0x2102 - UPD_RETVAL_BAD_REPLY
Dieser Fehler im Update-Modul kann auftreten, wenn die Internetverbindung über einen Proxyserver läuft, insbesondere den Webwasher-Proxy.

0x2104 - UPD_RETVAL_SERVER_ERROR
Dieser Fehler im Update-Modul gibt an, dass ein HTTP-Fehlercode über 500 vorliegt. Bei Verwendung des ESET HTTP-Servers weist Fehler 500 auf ein Problem mit der Speicherallokation hin.

0x2105 - UPD_RETVAL_INTERRUPTED
Dieser Fehler im Update-Modul kann auftreten, wenn die Internetverbindung über einen Proxyserver läuft, insbesondere den Webwasher-Proxy.

10.3 Fehlerdiagnose bei Problemen mit ERAS

Wenn Sie vermuten, dass ein Problem mit ERAS vorliegt, oder wenn das Programm nicht korrekt funktioniert, sollten Sie die folgenden Schritte durchführen:

1) Überprüfen Sie das ERAS-Log: Klicken Sie im Hauptmenü von ERAC auf **Extras** > **Serveroptionen**. Das Dialogfenster **Serveroptionen** wird angezeigt. Klicken Sie auf die Registerkarte **Logging** und dann auf **Log anzeigen**.

2) Wenn Sie keine Fehlermeldungen sehen, erhöhen Sie die Einstellung **Log-Umfang** im Dialogfenster **Serveroptionen** auf Stufe 5. (Im Anschluss an die Problemdiagnose sollten Sie den ursprünglichen Wert wiederherstellen.)

3) Für die Problemdiagnose kann es auch helfen, das Datenbank-Debug-Log auf derselben Registerkarte zu aktivieren. Nähere Informationen finden Sie im Abschnitt **Debug-Log**. Das Debug-Log sollte nur zum Reproduzieren von Problemen aktiviert und anschließend wieder abgeschaltet werden.

4) Sollte ein nicht in dieser Dokumentation aufgeführter Fehlercode erscheinen, wenden Sie sich bitte an den ESET-Support. Bitte beschreiben Sie, was für ein Problem vorliegt, wie es reproduziert oder ggf. umgangen werden kann. Nennen Sie unbedingt auch die Programmversionen aller beteiligten ESET Security-Produkte (ERAS, ERAC, ESET

Smart Security, ESET NOD32 Antivirus).

11. Tipps und Tricks

11.1 Taskplaner

ESET NOD32 Antivirus und ESET Smart Security verfügen über einen integrierten Taskplaner, mit dem regelmäßige Scans, Updates usw. eingerichtet werden können. Alle geplanten Tasks werden in diesem Taskplaner aufgeführt.

Die folgenden Tasktypen können über ERA konfiguriert werden:

- Start externer Anwendung
- Log-Wartung
- Prüfen des Computers
- Snapshot des Computerstatus erstellen
- Update
- Prüfung Systemstartdateien

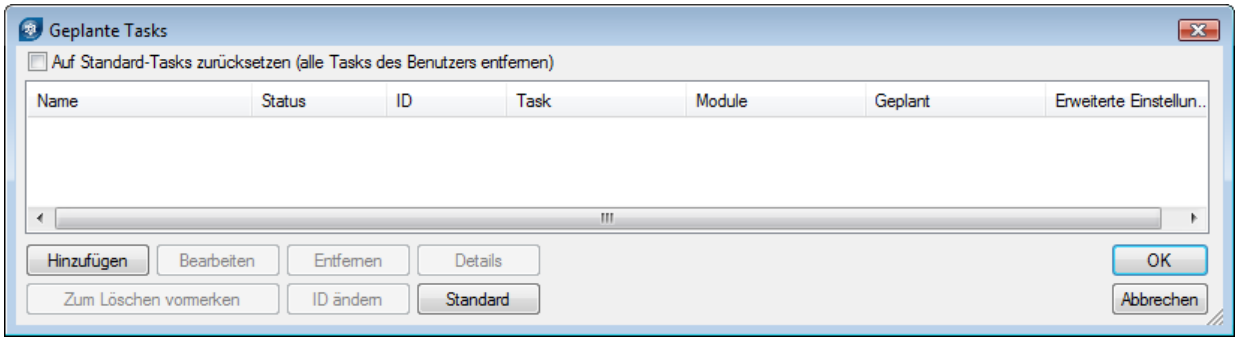
Tasks des Typs **Start externer Anwendung** müssen nur sehr selten eingerichtet werden. Der Task **Prüfung Systemstartdateien** ist ein Standardtask, dessen Parameter nach Möglichkeit nicht geändert werden sollten. Sofern nach der Installation keine Änderungen vorgenommen wurden, sind in ESET NOD32 und ESET Smart Security zwei vordefinierte Tasks dieses Typs konfiguriert. Mit dem ersten Task werden die Systemstartdateien nach jeder Anmeldung eines Benutzers geprüft, mit dem zweiten Task nach jedem erfolgreichen Update der Signaturdatenbank. Als Administrator werden Sie vermutlich am häufigsten mit den Tasktypen **Prüfen des Computers** und **Update** arbeiten:

- **Prüfen des Computers**
  Hiermit können Sie einen regelmäßigen Scan auf den Clients einrichten (in der Regel für die lokalen Datenträger).

- **Update**
  Dieser Tasktyp dient dazu, die ESET Clientlösungen auf den neuesten Stand zu halten. Es handelt sich hierbei um einen vordefinierten Task, der standardmäßig alle 60 Minuten ausgeführt wird. In der Regel wird es keinen Anlass geben, seine Parameter zu ändern. Die einzige Ausnahme bilden Notebooks, die oft außerhalb des Firmen-LANs eingesetzt werden, allerdings weiterhin über eine Internetverbindung verfügen. Hier kann der Update-Task so eingerichtet werden, dass er zwei Update-Profile nacheinander verwendet. So können die Notebooks zunächst versuchen, Updates über den lokalen Mirror-Server zu beziehen; wenn dies fehlschlägt, werden die Updates von den ESET-Update-Servern heruntergeladen.

Die Taskplaner-Konfiguration finden Sie auch im **ESET Configuration Editor** unter ESET Smart Security / ESET NOD32 Antivirus **>** **ESET-Kernel** > **Einstellungen** > **Taskplaner** > **Taskplaner** > **Bearbeiten**.

Nähere Informationen finden Sie im Kapitel ESET Configuration Editor 32.



Das Dialogfenster enthält unter Umständen bereits vorhandene Tasks (die Sie durch Klicken auf **Bearbeiten** bearbeiten können), eventuell ist es jedoch auch leer. Dies hängt davon ab, ob Sie eine Konfiguration von einem (zuvor bereits konfigurierten) Client geöffnet oder eine neue Datei mit der Standardvorlage erstellt haben, die keine Tasks enthält.

Jeder neue Task erhält eine ID-Nummer. Bei Standardtasks ist dies eine Dezimalzahl (1, 2, 3...), bei benutzerdefinierten Tasks ein hexadezimaler Schlüssel (z. B. *4AE13D6C*), der beim Erstellen des neuen Tasks automatisch erzeugt wird.

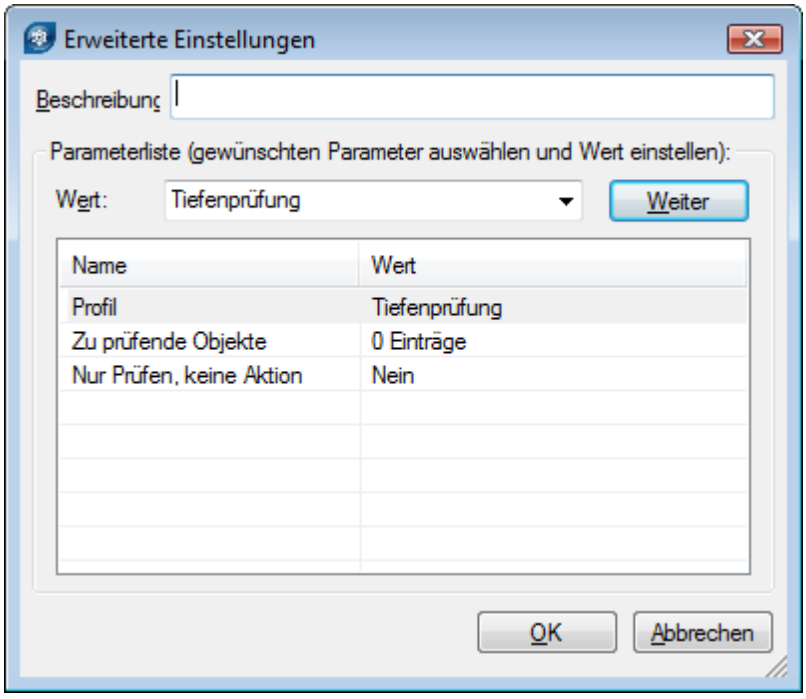
Wenn das Kontrollkästchen eines Tasks aktiviert ist, bedeutet dies, dass der Task aktiv ist und auf dem jeweiligen Client ausgeführt wird.

Die Schaltflächen im Dialogfenster „Geplante Tasks“ haben die folgenden Funktionen:

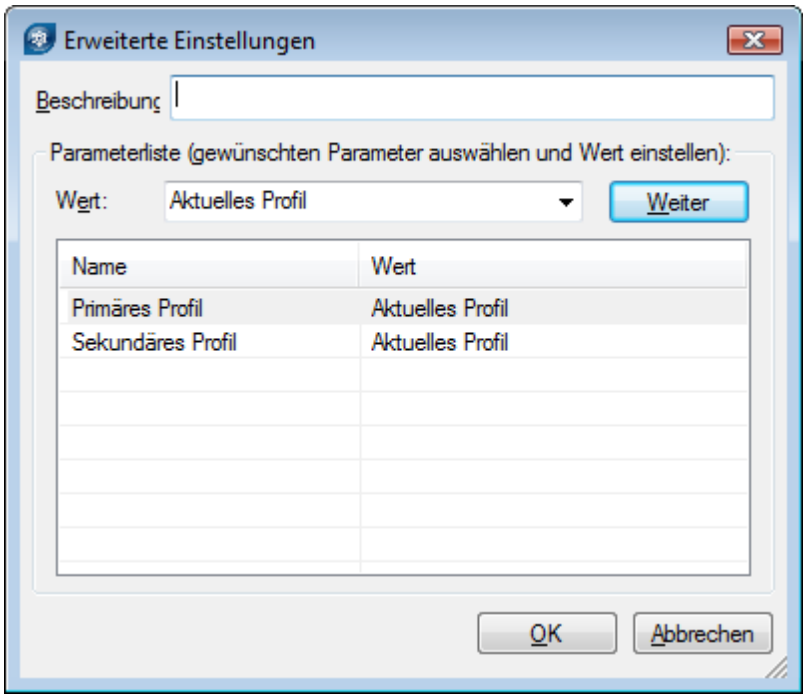
- **Hinzufügen** - Neuen Task hinzufügen
- **Bearbeiten** - Änderungen am ausgewählten Task vornehmen
- **ID ändern** - ID des ausgewählten Tasks ändern
- **Details** - Überblicksinformationen zum ausgewählten Task
- **Zum Löschen vormerken** - Bewirkt, dass Tasks mit derselben ID-Nummer wie der ausgewählte Task bei der Übernahme der *.xml*-Konfigurationsdatei von den Zielclients gelöscht werden.
- **Entfernen** - Ausgewählte Tasks aus der Liste entfernen. Bitte beachten Sie: Tasks werden hiermit lediglich aus der Liste in der .xml-Konfigurationsdatei entfernt, nicht jedoch auf den Zielclients gelöscht.

Beim Erstellen eines neuen Tasks (Schaltfläche **Hinzufügen**) bzw. beim Bearbeiten eines vorhandenen Tasks (**Bearbeiten**) müssen Sie festlegen, wann dieser ausgeführt werden soll. Dies kann entweder in einem bestimmten Intervall (jeden Tag um 12 Uhr, jeden Freitag usw.) oder ausgelöst durch ein bestimmtes Ereignis geschehen (nach einem erfolgreichen Update, beim ersten Computerstart am Tag usw.).

Bei einem Task des Typs **Prüfen des Computers** wird im letzten Schritt ein Fenster mit erweiterten Einstellungen angezeigt. Hier können Sie festlegen, welche Konfiguration (Scanprofil und zu prüfende Objekte) für den Scan verwendet werden soll.



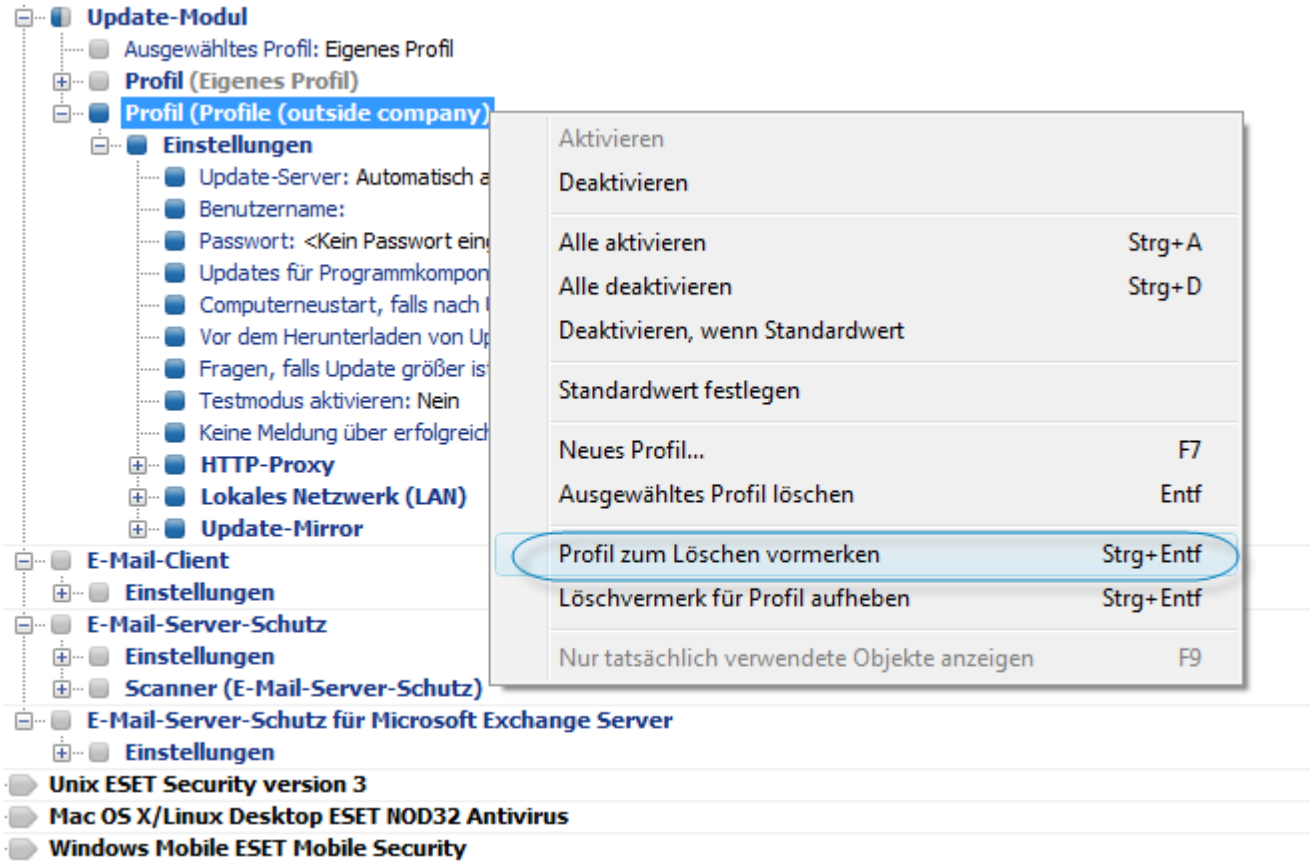
Bei einem Task des Typs **Update** geben Sie im letzten Schritt an, welche Update-Profile für den Task verwendet werden sollen. Es handelt sich hierbei um einen vordefinierten Task, der standardmäßig alle 60 Minuten ausgeführt wird. In der Regel wird es keinen Anlass geben, seine Parameter zu ändern. Die einzige Ausnahme bilden Notebooks, die oft außerhalb des Firmen-LANs eingesetzt werden, allerdings weiterhin über eine Internetverbindung verfügen. Für solche Geräte können Sie in diesem letzten Dialogfenster zwei unterschiedliche Update-Profile auswählen. So können die Notebooks zunächst versuchen, Updates über den lokalen Mirror-Server zu beziehen; wenn dies fehlschlägt, werden die Updates von den ESET-Update-Servern heruntergeladen.



11.2 Entfernen vorhandener Profile

Von Zeit zu Zeit stoßen Sie vielleicht auf Profile (für Updates oder Scans), die aus Versehen doppelt erstellt wurden. Um solche Dubletten per Remoteverwaltung zu entfernen, ohne andere Einstellungen im Taskplaner zu beeinflussen, gehen Sie wie folgt vor:

- Klicken Sie in ERAC auf die Registerkarte **Clients** und doppelklicken Sie auf einen betroffenen Client.
- Das Dialogfenster **Eigenschaften** für den Client wird angezeigt. Klicken Sie auf die Registerkarte **Konfiguration**. Aktivieren Sie die Optionen **Datei anschließend im ESET Configuration Editor zum Bearbeiten öffnen** sowie **Heruntergeladene Konfiguration im neuen Konfigurations-Task verwenden** und klicken Sie dann auf **Neuer Task**.
- Klicken Sie im Assistenten für den neuen Task auf **Bearbeiten**.
- Drücken Sie im Configuration Editor **Strg+D**, um alle Einstellungen abzuwählen, sodass sie grau erscheinen. So vermeiden Sie versehentliche Änderungen, da alle neuen Änderungen blau hervorgehoben werden.
- Klicken Sie mit der rechten Maustaste auf das zu entfernende Profil und wählen Sie im Kontextmenü den Befehl **Profil zum Löschen vormerken**. Dies bewirkt, dass das Profil gelöscht wird, sobald der Task auf den betreffenden Client übertragen wird.



- Klicken Sie im ESET Configuration Editor auf **Zurück zur Konsole** und speichern Sie die Änderungen.
- Vergewissern Sie sich, dass der ausgewählte Client in der Liste **Ausgewählte Objekte** im rechten Teil des Fensters enthalten ist. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

11.3 Exportieren einer Clientkonfiguration ins XML-Format und Verwendungsmöglichkeiten

Wählen Sie in ERAC einen beliebigen Client auf der Registerkarte **Clients** aus. Drücken Sie die rechte Maustaste und wählen Sie im Kontextmenü den Befehl **Konfiguration**. Klicken Sie auf **Speichern unter**, um die aktuelle Konfiguration des betreffenden Clients in eine *.xml*-Datei zu exportieren. (Über die Oberfläche von ESET Smart Security können Sie eine *.xml*-Konfigurationsdatei auch direkt exportieren.) Für die so erstellte *.xml*-Datei gibt es anschließend verschiedene Verwendungsmöglichkeiten:

- Sie können die *.xml*-Datei als fertige Konfiguration bei einer Remoteinstallation verwenden. So müssen Sie keine neue *.xml*-Datei erstellen, sondern weisen einfach dem neuen Installationspaket die vorhandene *.xml*-Datei zu (über die Schaltfläche **Auswählen**). Über die Oberfläche von ESET Smart Security können Sie *.xml*-Konfigurationsdateien auch direkt exportieren.

- Zur Konfiguration mehrerer Clients auf einmal können die ausgewählten Clients eine zuvor heruntergeladene *.xml*-Datei erhalten und die darin definierten Einstellungen übernehmen. Es wird also keine neue Konfiguration erstellt, sondern lediglich über die Schaltfläche **Auswählen** eine vorhandene Konfiguration zugewiesen.

Beispiel
Ein ESET Security-Produkt ist nur auf einem einzigen Arbeitsplatzrechner installiert. Nun können Sie über die Benutzeroberfläche des Programms direkt die gewünschte Konfiguration einrichten. Anschließend exportieren Sie die Einstellungen in eine *.xml*-Datei. Diese *.xml*-Datei können Sie dann zur Remoteinstallation auf anderen Arbeitsplatzrechnern verwenden. Diese Methode kann insbesondere für Aufgaben wie das Feinabstimmen von Firewall-Regeln im regelbasierten Modus sehr hilfreich sein.

11.4 Kombinierter Update-Abruf für Notebooks

Wenn Ihr Netzwerk auch Notebooks oder andere Mobilrechner umfasst, empfiehlt es sich, einen kombinierten Update-Abruf aus zwei Quellen zu konfigurieren: zum einen von den ESET-Update-Servern, zum anderen vom lokalen Mirror-Server. Die Notebooks versuchen dann zunächst, eine Verbindung zum lokalen Mirror-Server aufzubauen. Wenn dies nicht funktioniert, weil sie nicht im Firmennetz sind, werden die Updates direkt von den ESET-Servern heruntergeladen. Um diese Funktion einzurichten, gehen Sie wie folgt vor:

- Erstellen Sie zwei Update-Profile (siehe Exportieren einer Clientkonfiguration ins XML-Format und Verwendungsmöglichkeiten 97). Beim ersten (im folgenden Beispiel als „LAN" bezeichnet) werden die Updates vom Mirror-Server heruntergeladen, beim zweiten (im Folgenden „INET") von den ESET-Update-Servern.

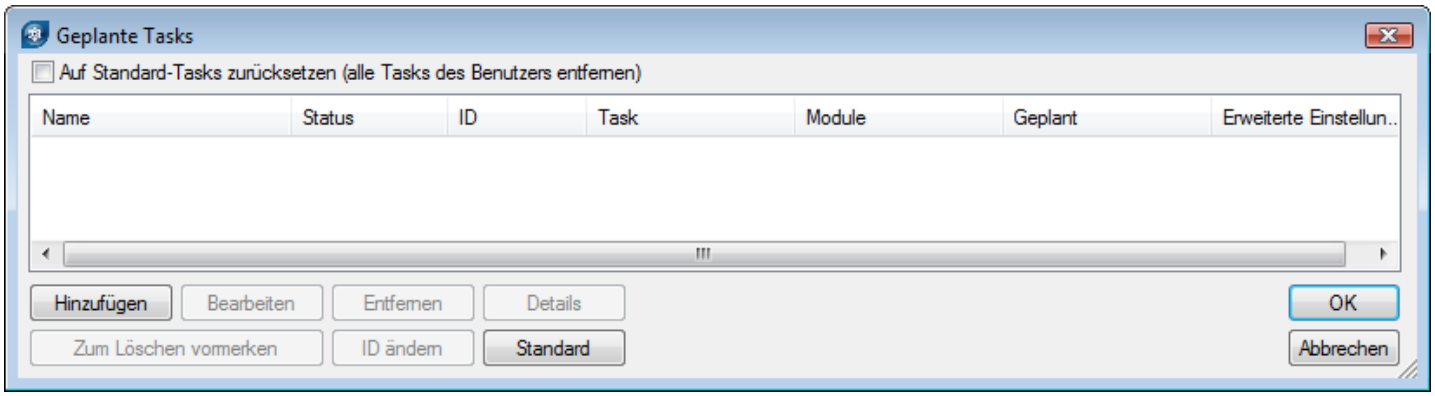
- Erstellen Sie über den Taskplaner einen neuen Update-Task oder bearbeiten Sie einen vorhandenen Task (**Tools** > **Taskplaner** im Hauptfenster von ESET Smart Security bzw. ESET NOD32 Antivirus).

Die Konfiguration kann direkt auf den Notebooks oder per Remoteverwaltung über den ESET Configuration Editor erstellt werden. Angewendet wird sie dann entweder bei der Installation oder per Konfigurations-Task zu einem beliebigen späteren Zeitpunkt.

Zum Erstellen neuer Profile im ESET Configuration Editor klicken Sie mit der rechten Maustaste auf den Zweig **Update** und wählen **Neues Profil** im Kontextmenü.

Das Ergebnis Ihrer Änderungen sollte etwa wie folgt aussehen:

Mit dem Profil „LAN" werden Updates vom Mirror-Server im Firmen-LAN heruntergeladen (*http://server:2221*), mit dem Profil „INET" dagegen von den ESET-Servern (**Automatisch auswählen**). Als nächstes definieren Sie einen Update-Task, der die beiden Update-Profile nacheinander ausführt. Hierzu wählen Sie im ESET Configuration Editor den Eintrag **ESET Smart Security**, **ESET NOD32 Antivirus** > **Kernel** > **Einstellungen** > **Taskplaner** aus. Klicken Sie auf **Bearbeiten**, um das Dialogfenster **Geplante Tasks** zu öffnen.



Um einen neuen Task zu erstellen, klicken Sie auf **Hinzufügen**. Wählen Sie in der Liste **Geplanter Task** den Typ **Update** aus und klicken Sie auf **Weiter**. Geben Sie den **Tasknamen** ein (z. B. *„Kombiniertes Update“*), wählen Sie **Regelmäßig - alle 60 Minuten** und wählen Sie dann das primäre und sekundäre Profil aus.

Wenn die Notebooks zuerst versuchen sollen, den Mirror-Server zu erreichen, richten Sie „LAN“ als primäres und „INET“ als sekundäres Profil ein. Das Profil „INET“ kommt dann nur zum Einsatz, wenn das Update über das Profil „LAN“ fehlschlägt.

Empfehlung: Exportieren Sie die aktuelle *.xml*-Konfiguration eines Clients (nähere Informationen siehe Fehlerdiagnose bei Problemen mit ERAS 92) und nehmen Sie die oben beschriebenen Änderungen an der exportierten *.xml*-Datei vor. So verhindern Sie doppelt angelegte Tasks im Taskplaner sowie nicht funktionierende Profile.

11.5 Installation von Produkten anderer Hersteller über ERA

Neben einer Remoteinstallation von ESET Produkten kann ESET Remote Administrator auch andere Programme installieren. Hierzu muss das gewünschte Installationspaket lediglich im Format *.msi* vorliegen. Die Remoteinstallation eines benutzerdefinierten Pakets läuft sehr ähnlich ab wie im Kapitel Remoteinstallation 36 beschrieben.

Der wesentliche Unterschied liegt in der Erstellung des Pakets. Hierzu gehen Sie wie folgt vor:

1) Klicken Sie in ERAC auf die Registerkarte **Remoteinstallation**.
2) Klicken Sie auf die Schaltfläche **Pakete**.
3) Wählen Sie in der Liste **Typ** den Typ **Benutzerdefiniertes Paket**.
4) Klicken Sie auf **Erstellen**, dann auf **Datei hinzufügen** und wählen Sie die gewünschte *.msi*-Paketdatei aus.
5) Wählen Sie in der Liste **Einstiegsdatei** die gewünschte Datei aus und klicken Sie auf **Erstellen**.
6) Im ursprünglichen Dialogfenster können Sie nun Befehlszeilenparameter für die *.msi*-Datei angeben. Verwenden Sie hierfür dieselben Parameter wie bei einer lokalen Installation des Pakets.
7) Klicken Sie auf **Speichern unter**, um das Paket zu speichern.
8) Klicken Sie auf **Schließen**, um den Installationspaket-Editor zu schließen.

Das neue benutzerdefinierte Paket kann genau wie in den vorhergehenden Kapiteln beschrieben per Remoteinstallation auf den Client-Arbeitsplatzrechnern installiert werden. Hierzu wird es zunächst wie gewohnt per Push-Installation, per Anmeldeskript oder E-Mail auf die Zielrechner übermittelt. Nach dem Start des Pakets übernimmt der Microsoft Windows Installer-Dienst die restlichen Installationsaufgaben.

12. ESET SysInspector

12.1 Einführung in ESET SysInspector

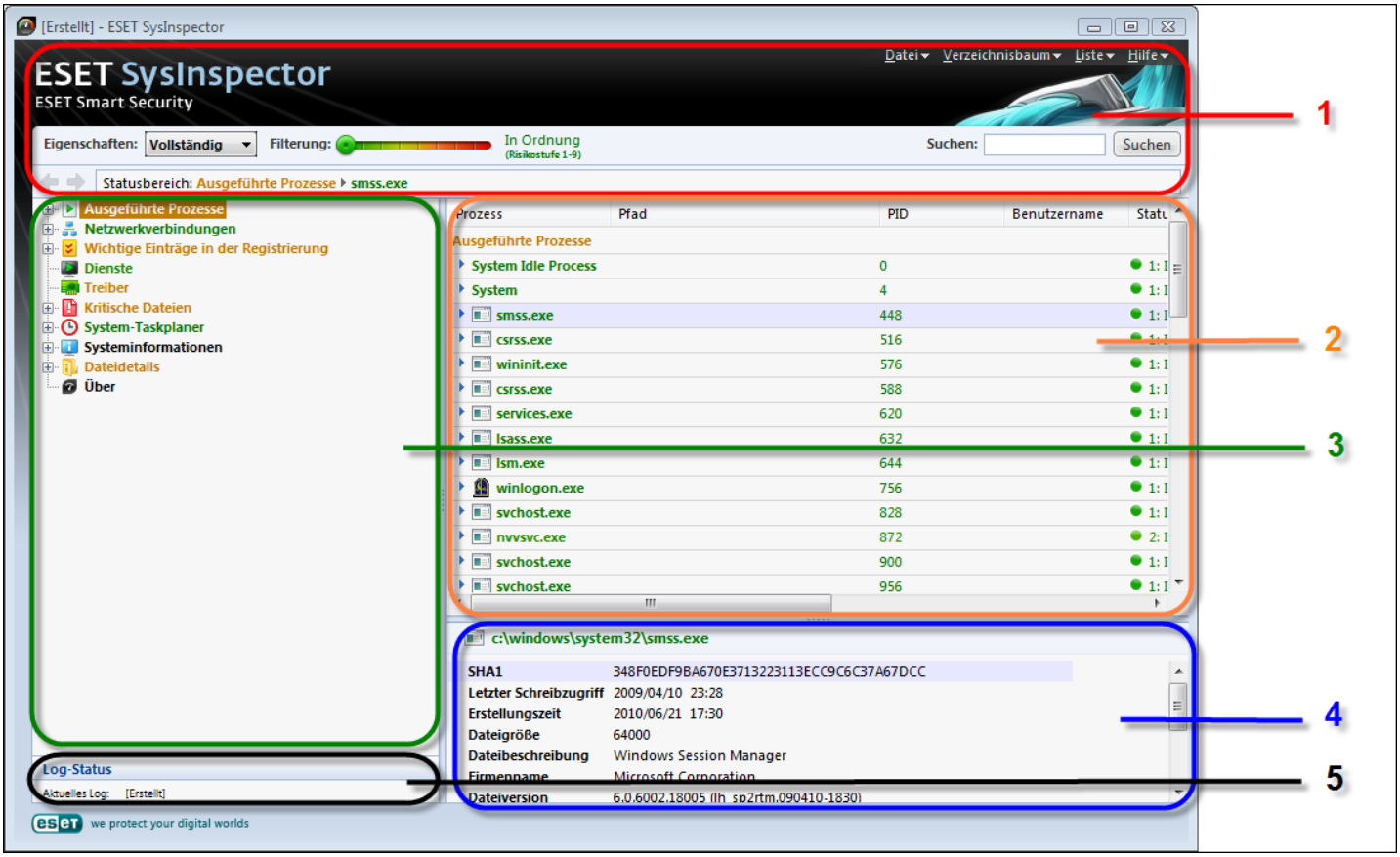
ESET SysInspector ist eine Diagnoseanwendung, mit der Sie umfassende Informationen zu einem bestimmten Computer anzeigen können, etwa zu installierten Treibern und Anwendungen, Netzwerkverbindungen oder wichtigen Registrierungseinträgen. Diese Angaben helfen Ihnen bei der Problemdiagnose, wenn sich ein System nicht wie erwartet verhält - ob dies nun an einer Inkompatibilität (Software/Hardware) oder an einer Malware-Infektion liegt.

12.1.1 Starten von ESET SysInspector

Zum Starten von ESET SysInspector führen Sie einfach die von der ESET-Website heruntergeladene Programmdatei *SysInspector.exe* aus. Wenn bereits ein ESET Security-Produkt installiert ist, können Sie ESET SysInspector direkt aus dem Startmenü starten (Programme > ESET > ...). Bitte haben Sie einen Augenblick Geduld, während die Anwendung Ihr System untersucht. Je nach der Art der Hardwarekonfiguration und den zu erfassenden Daten kann dies einige Minuten dauern.

12.2 Benutzeroberfläche und Bedienung

Zur einfachen Bedienung ist das Hauptfenster in vier Bereiche gegliedert. Am oberen Rand befindet sich ein Bereich mit dem Menü und sonstigen Bedienelementen (1). Links finden Sie den Navigationsbereich (3), rechts in der Mitte den Beschreibungsbereich (2) und rechts unten den Detailbereich (4). Der Bereich „Log-Status" (5) zeigt die grundlegenden Eigenschaften eines Logs (verwendeter Filter, Filtertyp, Ergebnis eines Vergleichs?, usw.).



12.2.1 Menüs und Bedienelemente

Dieser Abschnitt beschreibt die Menüs und sonstigen Bedienelemente in ESET SysInspector.

Datei
Über dieses Menü können Sie die aktuellen Systeminformationen zur späteren Untersuchung speichern oder ein zuvor gespeichertes Log wieder öffnen. Falls ein Log weitergegeben werden soll, sollten Sie es über die Funktion **Zum Senden geeignet** erstellen. Sicherheitsrelevante Daten (Name und Berechtigungen des aktuellen Benutzers, Computername, Domänenname, Umgebungsvariablen usw.) werden dann nicht in das Log aufgenommen.

HINWEIS: Gespeicherte ESET SysInspector-Logs können Sie schnell wieder öffnen, indem Sie sie einfach auf das Hauptfenster ziehen und dort ablegen.

Verzeichnisbaum
Hiermit können Sie alle Knoten erweitern oder schließen sowie die ausgewählten Bereiche in ein Dienste-Skript exportieren.

Liste
Dieses Menü enthält Funktionen zur einfacheren Navigation im Programm sowie eine Reihe von Zusatzfunktionen, etwa für die Online-Informationssuche.

Hilfe
Über dieses Menü finden Sie Informationen zur Anwendung und ihren Funktionen.

Eigenschaften
Legt fest, welche Informationen in den anderen Bereichen des Hauptfensters angezeigt werden. Hiermit können Sie sich die Bedienung des Programms übersichtlicher gestalten. Im Modus „Einfach" werden die Informationen angezeigt, die Sie benötigen, um gängige Probleme mit dem System zu lösen. Im Modus „Mittel" sehen Sie auch weniger häufig benötigte Informationen. Im Modus „Vollständig" zeigt ESET SysInspector alle verfügbaren Informationen an, sodass Sie auch sehr spezielle Probleme beheben können.

Filterung
Mit der Filterfunktion können Sie schnell verdächtige Dateien oder Registrierungseinträge auf Ihrem System finden. Durch Verschieben des Schiebereglers legen Sie fest, ab welcher Risikostufe Objekte angezeigt werden. Wenn der Schieberegler ganz links steht (Risikostufe 1), werden alle Objekte angezeigt. Steht der Schieberegler hingegen weiter rechts, werden alle Objekte unterhalb der eingestellten Risikostufe ausgeblendet, sodass Sie nur die Objekte ab einer bestimmten Risikostufe sehen. Wenn der Schieberegler ganz rechts steht, sehen Sie nur solche Objekte, die bekanntermaßen schädlich sind.

Alle Objekte mit einer Risikostufe von 6 bis 9 können ein Sicherheitsrisiko darstellen. Falls solche Objekte auf Ihrem System gefunden werden und Sie keine ESET Security-Lösung einsetzen, empfiehlt sich eine Überprüfung Ihres Systems mit dem kostenlosen ESET Online Scanner.

HINWEIS: Um schnell herauszufinden, welche Risikostufe ein bestimmtes Objekt hat, vergleichen Sie einfach seine Farbe mit den Farben auf dem Schieberegler für die Risikostufe.

Suchen
Mit der Suche können Sie ein bestimmtes Objekt schnell über seinen Namen (oder einen Teil des Namens) finden. Die Ergebnisse der Suchanfrage werden im Beschreibungsbereich angezeigt.

Zurück/Vor
Über die Schaltflächen mit den Pfeilen nach links und rechts können Sie zwischen den bisherigen Anzeigeinhalten des Beschreibungsbereichs wechseln. Anstatt auf die Pfeilschaltflächen zu klicken, können Sie auch einfach die Rück- bzw. Leertaste drücken.

Statusbereich
Hier sehen Sie, welcher Knoten im Navigationsbereich gerade ausgewählt ist.

Wichtig: Rot hervorgehobene Objekte sind unbekannt und werden daher als potenziell gefährlich markiert. Dies bedeutet jedoch nicht automatisch, dass Sie die Datei gefahrlos löschen können. Vergewissern Sie sich vor dem Löschen auf jeden Fall, dass die Datei tatsächlich überflüssig ist bzw. dass von ihr eine Gefahr ausgeht.

12.2.2 Navigation in ESET SysInspector

In ESET SysInspector gliedern sich die unterschiedlichen Systeminformationen in eine Reihe von Hauptabschnitten, die so genannten „Knoten". Wenn zu einem Knoten weitere Details vorhanden sind, können Sie ihn erweitern (ausklappen), um seine Unterknoten anzuzeigen. Zum Erweitern oder Reduzieren (Einklappen) eines Knotens doppelklicken Sie einfach darauf oder klicken auf das Symbol ⊞ bzw. ⊟ neben seinem Namen. Soweit vorhanden, werden im Beschreibungsbereich Detailinhalte zum gerade im Navigationsbereich ausgewählten Knoten angezeigt. Diese Einträge im Beschreibungsbereich können Sie dann wiederum auswählen, um (soweit vorhanden) im Detailbereich weitere Detailinformationen dazu anzuzeigen.

Im Folgenden sind die Hauptknoten im Navigationsbereich sowie die dazugehörigen Informationen im Beschreibungs- und Detailbereich beschrieben.

Ausgeführte Prozesse
Dieser Knoten enthält Informationen zu den Anwendungen und Prozessen, die zum Zeitpunkt der Log-Erstellung ausgeführt wurden. Das Beschreibungsfenster zeigt weitere Details zu jedem Prozess, etwa die verwendeten dynamischen Bibliotheken samt Speicherort, den Namen des Programmherstellers, die Risikostufe der Dateien usw.

Wenn Sie einen Eintrag im Beschreibungsfenster auswählen, erscheinen im Detailfenster weitere Informationen wie z. B. die Größe oder der Hashwert der betreffenden Datei.

HINWEIS: Jedes Betriebssystem enthält eine Reihe zentraler Kernelkomponenten, die ständig ausgeführt werden und wichtige Funktionen für andere Anwendungen bereitstellen. In bestimmten Fällen wird für solche Prozesse in ESET SysInspector ein Dateipfad angezeigt, der mit \??\ beginnt. Dies bedeutet, dass die Security-Software vor dem Start für diese Prozesse optimiert wird; ihre Ausführung ist legitim, und sie stellen kein Risiko für die Systemsicherheit dar.

Netzwerkverbindungen
Wenn Sie im Navigationsbereich ein Protokoll (TCP oder UDP) auswählen, erscheint im Beschreibungsbereich eine Liste der Prozesse und Anwendungen, die über das betreffende Protokoll im Netzwerk kommunizieren, samt der jeweiligen Remoteadresse. Außerdem können Sie hier die IP-Adressen der DNS-Server überprüfen.

Wenn Sie einen Eintrag im Beschreibungsfenster auswählen, erscheinen im Detailfenster weitere Informationen wie z. B. die Größe oder der Hashwert der betreffenden Datei.

Wichtige Einträge in der Registrierung
Hier finden Sie eine Liste ausgewählter Registrierungseinträge, die oft im Zusammenhang mit Systemproblemen stehen. Dies betrifft beispielsweise die Registrierungseinträge für Autostart-Programme, Browser-Hilfsobjekte (BHO) usw.

Im Beschreibungsbereich werden die mit dem jeweiligen Registrierungseintrag verbundenen Dateien angezeigt. Im Detailbereich finden Sie dazu weitere Informationen.

Dienste
Bei diesem Knoten enthält der Beschreibungsbereich eine Liste der Dateien, die als Windows-Dienste registriert sind. Im Detailbereich sind die Ausführungsart des Dienstes sowie weitere Informationen zur Datei angegeben.

Treiber
Liste der im System installierten Treiber

Kritische Dateien
Unter diesem Knoten können Sie sich im Beschreibungsbereich den Inhalt wichtiger Konfigurationsdateien von Microsoft Windows anzeigen lassen.

Systeminformationen
Hier finden Sie ausführliche Informationen zu Hardware und Software, den gesetzten Umgebungsvariablen sowie den Benutzerberechtigungen.

Dateidetails
Dieser Knoten enthält eine Liste der wichtigen Systemdateien sowie der Dateien im Ordner „Programme". Im Beschreibungs- und Detailbereich finden Sie weitere Informationen zu den einzelnen Dateien.

Über
Informationen zu ESET SysInspector

12.2.3 Vergleichsfunktion

Mit der Funktion „Vergleichen" können Sie zwei vorhandene Logs vergleichen. Als Ergebnis werden die Unterschiede zurückgegeben, also die Einträge, die nicht in beiden Logs enthalten sind. Diese Funktion ist sehr praktisch, um Änderungen am System zu erkennen, etwa infolge der Aktivitäten eines Schadprogramms.

Nach dem Start erzeugt die Anwendung ein neues Log, das in einem neuen Fenster angezeigt wird. Um das Log zu speichern, klicken Sie auf **Datei** -> **Log speichern**. Gespeicherte Log-Dateien können Sie später wieder öffnen, um sie einzusehen. Hierzu verwenden Sie den Befehl **Datei** -> **Log öffnen**. Im Hauptfenster von ESET SysInspector wird immer nur jeweils ein Log angezeigt.

Beim Vergleich zweier Logs vergleichen Sie grundsätzlich das gerade aktive Log mit einem gespeicherten Log aus einer Datei. Hierzu klicken Sie auf **Datei** -> **Log vergleichen** und wählen dann **Datei auswählen**. Das ausgewählte Log wird nun mit dem aktiven (im Programmfenster angezeigten) Log verglichen. Das Ergebnis (ein so genanntes „Vergleichs-Log") zeigt nur die Unterschiede zwischen den beiden Logs.

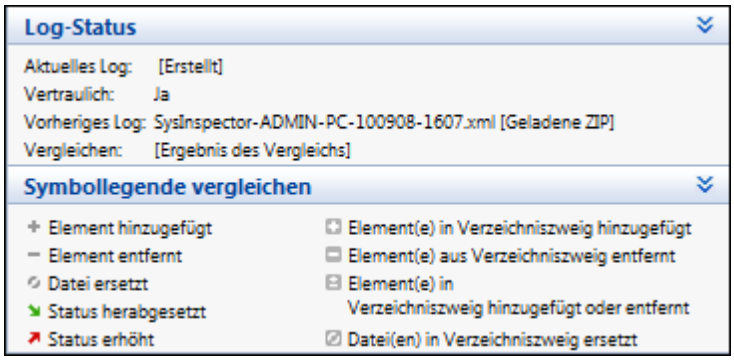
HINWEIS: Wenn Sie nach dem Vergleich zweier Logs auf **Datei** -> **Log speichern** klicken und das Ergebnis als ZIP-Datei speichern, werden beide Log-Dateien gespeichert. Wenn Sie die so entstandene Datei später öffnen, werden die enthaltenen Logs automatisch verglichen.

Neben den einzelnen Einträgen erscheinen Symbole, die angeben, um was für eine Art von Unterschied es sich handelt. Einträge mit dem Symbol – sind nur im aktiven Log enthalten, nicht jedoch in dem gespeicherten Log aus der geöffneten Datei. Einträge mit + sind umgekehrt nur in dem Log aus der geöffneten Datei enthalten, nicht jedoch im aktiven Log.

Die einzelnen Symbole haben die folgende Bedeutung:

+ Neuer Wert, nicht im vorherigen Log enthalten
Betreffender Zweig der Baumstruktur enthält neue Werte
– Gelöschter Wert, nur im vorherigen Log enthalten
Betreffender Zweig der Baumstruktur enthält gelöschte Werte
Wert/Datei wurde geändert
Betreffender Zweig der Baumstruktur enthält geänderte Werte/Dateien
Risiko ist gesunken (war im vorherigen Log höher)
Risiko ist gestiegen (war im vorherigen Log niedriger)

Die Bedeutung aller Symbole sowie die Namen der verglichenen Logs werden auch in der Legende links unten im Programmfenster angezeigt.



Sie können jedes Vergleichs-Log in einer Datei speichern und später wieder öffnen.

Beispiel:

Erstellen und speichern Sie ein Log mit einem ersten Stand der Systeminformationen in einer Datei namens alt.xml. Nehmen Sie einige Änderungen am System vor und öffnen Sie dann SysInspector, um ein neues Log zu erstellen. Speichern Sie dieses unter dem Namen *neu.xml*.
Um die Unterschiede zwischen diesen beiden Logs zu sehen, klicken Sie auf **Datei** > **Logs vergleichen**. Das Programm erstellt so ein Vergleichs-Log, das die Unterschiede zwischen den beiden Logs zeigt.

Dasselbe Ergebnis erzielen Sie bei einem Aufruf über die Befehlszeile mit den folgenden Parametern:

SysIsnpector.exe neu.xml alt.xml

12.3 Befehlszeilenparameter

Mit ESET SysInspector können Sie auch von der Befehlszeile aus Berichte erzeugen. Hierzu stehen die folgenden Parameter zur Verfügung:

/gen	Ergebnis-Log direkt aus der Befehlszeile erzeugen, keine grafische Oberfläche anzeigen
/privacy	Keine sicherheitsrelevanten Informationen ins Log aufnehmen
/zip	Ergebnis-Log direkt in einer komprimierten Datei auf dem Datenträger speichern
/silent	Keine Fortschrittsleiste während der Erstellung des Logs anzeigen
/help, **/?**	Hilfe zu den Befehlszeilenparametern anzeigen

Beispiele

Bestimmtes Log direkt in den Browser laden: *SysInspector.exe "c:\clientlog.xml"*
Log im aktuellen Ordner speichern: *SysInspector.exe /gen*
Log in einem bestimmten Ordner speichern: *SysInspector.exe /gen="c:\ordner\"*
Log in einer bestimmten Datei speichern: *SysInspector.exe /gen="c:\ordner\meinlog.xml"*
Log ohne sicherheitsrelevante Daten direkt in einer komprimierten Datei speichern: *SysInspector.exe /gen="c:\meinlog.zip" /privacy /zip*
Zwei Logs vergleichen: *SysInspector.exe "log_neu.xml" "log_alt.xml"*

HINWEIS: Datei- und Ordnernamen mit Leerzeichen sollten in Hochkommata gesetzt werden.

12.4 Dienste-Skript

Dienste-Skripte sind eine weitere praktische Funktion von ESET SysInspector. Hiermit können Sie unerwünschte Objekte vom System entfernen.

Über ein Dienste-Skript können Sie das gesamte SysInspector-Log oder ausgewählte Teile davon exportieren. Nach dem Export können Sie unerwünschte Objekte zum Löschen markieren. Anschließend können Sie das so bearbeitete Log ausführen, um die markierten Objekte zu löschen.

Dienste-Skripte sind für erfahrene Benutzer gedacht, die sich gut mit der Diagnose und Behebung von Systemproblemen auskennen. Andere Benutzer sollten davon Abstand nehmen, denn unbedachte Änderungen können dazu führen, dass das Betriebssystem unbrauchbar wird.

Beispiel:

Wenn Sie vermuten, dass Ihr Computer mit einem Virus infiziert ist, den Ihr Antivirusprogramm nicht erkennt, gehen Sie wie folgt vor:

- Führen Sie ESET SysInspector aus, um einen neuen System-Snapshot zu erstellen.
- Wählen Sie das erste Objekt im Navigationsbereich auf der linken Seite aus, halten Sie die Strg-Taste gedrückt und klicken Sie auf das letzte Objekt im Navigationsbereich, um den gesamten Inhalt zu markieren. Lassen Sie die Strg-Taste los.
- Klicken Sie mit der rechten Maustaste auf die ausgewählten Objekte und wählen Sie im Kontextmenü den Befehl **Ausgewählte Bereiche in das Dienste-Skript exportieren**.
- Die ausgewählten Objekte werden in ein neues Log exportiert.
- Sie kommen nun zum wichtigsten Schritt des gesamten Vorgangs: Öffnen Sie das neue Log und ändern Sie das Zeichen „-“ vor allen Objekten, die gelöscht werden sollen, auf „+“. Achten Sie dabei darauf, dass Sie keine Objekte markieren, die für den korrekten Systembetrieb erforderlich sind.
- Öffnen Sie ESET SysInspector, klicken Sie auf **Datei** > **Dienste-Skript ausführen** und wählen Sie Ihr Skript aus.
- Klicken Sie auf **OK**, um das Skript auszuführen.

12.4.1 Erstellen eines Dienste-Skripts

Um ein Skript zu erstellen, klicken Sie im SysInspector-Hauptfenster mit der rechten Maustaste auf ein beliebiges Element im Navigationsbereich auf der linken Seite des Fensters. Wählen Sie im Kontextmenü dann entweder **Alle Bereiche in das Dienste-Skript exportieren** oder **Ausgewählte Bereiche in das Dienste-Skript exportieren**.

HINWEIS: Wenn Sie gerade zwei Logs miteinander vergleichen, ist kein Export in ein Dienste-Skript möglich.

12.4.2 Aufbau des Dienste-Skripts

In der ersten Zeile des Skriptheaders finden Sie Angaben zur Engine-Version (ev), zur Version der Benutzeroberfläche (gv) sowie zur Log-Version (lv). Über diese Angaben können Sie mögliche Änderungen an der XML-Datei verfolgen, über die das Skript erzeugt wird, und dadurch Inkonsistenzen bei der Ausführung vermeiden. An diesem Teil des Skripts sollten keine Änderungen vorgenommen werden.

Der Rest der Datei gliedert sich in mehrere Abschnitte, deren Einträge Sie bearbeiten können, um festzulegen, welche davon bei der Ausführung verarbeitet werden sollen. Um einen Eintrag für die Verarbeitung zu markieren, ersetzen Sie das davor stehende Zeichen „-“ durch ein „+“. Die einzelnen Skriptabschnitte sind jeweils durch eine Leerzeile voneinander getrennt. Jeder Abschnitt hat eine Nummer und eine Überschrift.

01) Running processes (Ausgeführte Prozesse)

Dieser Abschnitt enthält eine Liste mit allen Prozessen, die auf dem System ausgeführt werden. Für jeden Prozess ist der UNC-Pfad gefolgt vom CRC16-Hashwert in Sternchen (*) aufgeführt.

Beispiel:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In diesem Beispiel wurde der Prozess module32.exe ausgewählt, indem er mit dem Zeichen „+“ markiert wurde. Beim Ausführen des Skripts wird dieser Prozess beendet.

02) Loaded modules (Geladene Module)

Dieser Abschnitt enthält eine Liste der momentan verwendeten Systemmodule.

Beispiel:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In diesem Beispiel wurde das Modul khbekhb.dll mit einem „+“ markiert. Beim Ausführen des Skripts werden alle Prozesse, die dieses Modul verwenden, ermittelt und anschließend beendet.

03) TCP connections (TCP-Verbindungen)

Dieser Abschnitt enthält Informationen zu den aktiven TCP-Verbindungen.

Beispiel:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Beim Ausführen des Skripts wird der Eigentümer des Sockets der markierten TCP-Verbindungen ermittelt. Anschließend wird der Socket beendet, wodurch Systemressourcen wieder frei werden.

04) UDP endpoints (UDP-Endpunkte)

Dieser Abschnitt enthält Informationen zu den aktiven UDP-Endpunkten.

Beispiel:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Beim Ausführen des Skripts wird der Eigentümer des Sockets der markierten UDP-Verbindungen ermittelt. Anschließend wird der Socket beendet.

05) DNS server entries (DNS-Servereinträge)

Dieser Abschnitt enthält Angaben zur aktuellen DNS-Serverkonfiguration.

Beispiel:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Beim Ausführen des Skripts werden die markierten DNS-Servereinträge entfernt.

06) Important registry entries (Wichtige Registrierungseinträge)

Dieser Abschnitt enthält Informationen zu wichtigen Registrierungseinträgen.

Beispiel:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Beim Ausführen des Skripts werden die markierten Einträge gelöscht, auf eine Länge von 0 Byte abgeschnitten oder auf die Standardwerte zurückgesetzt. Was davon im Einzelfall geschieht, hängt von der Art des Eintrags und dem Wert des Schlüssels ab.

07) Services (Dienste)

Dieser Abschnitt enthält eine Liste der auf dem System registrierten Dienste.

Beispiel:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Beim Ausführen des Skripts werden die markierten Dienste samt davon abhängiger Dienste beendet und deinstalliert.

08) Drivers (Treiber)

Dieser Abschnitt enthält eine Liste der installierten Treiber.

Beispiel:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Beim Ausführen des Skripts werden die Registrierungen der ausgewählten Treiber aufgehoben, und die Treiber werden vom System entfernt.

09) Critical files (Kritische Dateien)

Dieser Abschnitt enthält Angaben zu Dateien, die für eine korrekte Funktion des Betriebssystems wesentlich sind.

Beispiel:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[…]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[…]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[…]
```

Die ausgewählten Objekte werden entweder gelöscht oder auf ihren ursprünglichen Wert zurückgesetzt.

12.4.3 Ausführen von Dienste-Skripten

Markieren Sie die gewünschten Elemente, speichern und schließen Sie das Skript. Führen Sie das fertige Skript dann direkt aus dem SysInspector-Hauptfenster aus, indem Sie im Menü „Datei“ auf „Dienste-Skript ausführen“ klicken. Beim Öffnen eines Skripts wird die folgende Bestätigungsabfrage angezeigt: **Möchten Sie das Dienste-Skript „% Skriptname%“ wirklich ausführen?** Nachdem Sie diese Abfrage bestätigt haben, erscheint unter Umständen eine weitere Warnmeldung, dass das auszuführende Dienste-Skript nicht signiert wurde. Klicken Sie auf **Starten**, um das Skript auszuführen.

Nach erfolgreicher Ausführung des Skripts erscheint eine Bestätigungsmeldung.

Wenn das Skript nur teilweise verarbeitet werden konnte, wird ein Dialogfenster mit der folgenden Meldung angezeigt: **Das Dienste-Skript wurde teilweise ausgeführt. Möchten Sie den Fehlerbericht anzeigen?** Wählen Sie **Ja**, um einen ausführlichen Fehlerbericht mit Informationen zu den nicht ausgeführten Aktionen anzuzeigen.

Wenn das Skript nicht erkannt wurde, wird ein Dialogfenster mit der folgenden Meldung angezeigt: **Das ausgewählte Dienste-Skript trägt keine Signatur. Wenn Sie unbekannte Skripts und Skripte ohne Signatur ausführen, können die Daten Ihres Computers beschädigt werden. Möchten Sie das Skript und die Aktionen wirklich ausführen?** Eine solche Meldung kann durch Inkonsistenzen im Skript verursacht werden (beschädigter Header, beschädigte Abschnittsüberschrift, fehlende Leerzeile zwischen Bereichen usw.). Sie können dann entweder die Skriptdatei öffnen und die Fehler beheben oder ein neues Dienste-Skript erstellen.

12.5 Tastaturbefehle

Für die Arbeit mit ESET SysInspector stehen Ihnen die folgenden Tastaturbefehle zur Verfügung:

Datei

Strg+O	Vorhandenes Log öffnen
Strg+S	Erstelltes Log speichern

Erstellen

Strg+G	Standarduntersuchung des Systems
Strg+H	Systemuntersuchung, bei der auch sicherheitsrelevante Informationen protokolliert werden

Filterung

1, O	Risikostufe „In Ordnung" - Objekte mit Risikostufe 1-9 anzeigen
2	Risikostufe „In Ordnung" - Objekte mit Risikostufe 2-9 anzeigen
3	Risikostufe „In Ordnung" - Objekte mit Risikostufe 3-9 anzeigen
4, U	Risikostufe „Unbekannt" - Objekte mit Risikostufe 4-9 anzeigen
5	Risikostufe „Unbekannt" - Objekte mit Risikostufe 5-9 anzeigen
6	Risikostufe „Unbekannt" - Objekte mit Risikostufe 6-9 anzeigen
7, B	Risikostufe „Risikoreich" - Objekte mit Risikostufe 7-9 anzeigen
8	Risikostufe „Risikoreich" - Objekte mit Risikostufe 8-9 anzeigen
9	Risikostufe „Risikoreich" - Objekte mit Risikostufe 9 anzeigen
-	Risikostufe vermindern
+	Risikostufe erhöhen
Strg+9	Filtermodus: Objekte ab der jeweiligen Risikostufe anzeigen
Strg+0	Filtermodus: Nur Objekte mit der jeweiligen Risikostufe anzeigen

Anzeigen

Strg+5	Anzeige nach Hersteller - alle Hersteller
Strg+6	Anzeige nach Hersteller - nur Microsoft
Strg+7	Anzeige nach Hersteller - alle anderen Hersteller
Strg+3	Einstellung „Eigenschaften" auf „Vollständig" setzen
Strg+2	Einstellung „Eigenschaften" auf „Mittel" setzen
Strg+1	Einstellung „Eigenschaften" auf „Einfach" setzen
Rücktaste	Einen Schritt zurück
Leertaste	Einen Schritt weiter
Strg+W	Knoten erweitern (ausklappen)
Strg+Q	Knoten verkleinern (einklappen)

Diverse Befehle

Strg+T	Zur ursprünglichen Position eines in den Suchergebnissen ausgewählten Elements springen
Strg+P	Grundlegende Angaben zu einem Element anzeigen
Strg+A	Vollständige Angaben zu einem Element anzeigen
Strg+C	Daten/Baumpfad des aktuellen Elements kopieren
Strg+X	Elemente ausschneiden
Strg+B	Im Internet nach Informationen zur ausgewählten Datei suchen
Strg+L	Speicherordner der ausgewählten Datei öffnen
Strg+R	Betreffenden Eintrag im Registrierungseditor öffnen
Strg+Z	Dateipfad kopieren (wenn sich das Element auf eine Datei bezieht)
Strg+F	Zum Suchfeld wechseln
Strg+D	Suchergebnisse schließen
Strg+E	Dienste-Skript ausführen

Vergleich

Strg+Alt+O	Ursprüngliches Log/Vergleichs-Log öffnen
Strg+Alt+R	Vergleich schließen
Strg+Alt+1	Alle Elemente anzeigen
Strg+Alt+2	Nur hinzugefügte Elemente anzeigen (Elemente, die nur im aktuellen Log vorhanden sind)
Strg+Alt+3	Nur gelöschte Elemente anzeigen (Elemente, die nur im ursprünglichen Log vorhanden sind)
Strg+Alt+4	Nur ersetzte Elemente (inkl. Dateien) anzeigen
Strg+Alt+5	Nur Unterschiede zwischen den Logs anzeigen
Strg+Alt+C	Vergleich anzeigen
Strg+Alt+N	Aktuelles Log anzeigen
Strg+Alt+P	Ursprüngliches Log öffnen

Sonstige

F1	Hilfe anzeigen
Alt+F4	Programm beenden
Alt+Umschalt+F4	Programm ohne Rückfrage beenden
Strg+I	Log-Statistik anzeigen

12.6 Systemanforderungen

Für einen reibungslosen Betrieb von ESET SysInspector sollten die folgenden Hardware- und Softwareanforderungen erfüllt sein:

Windows 2000, XP, 2003
400-MHz-Prozessor, 32 Bit (x86) / 64 Bit (x64)
128 MB RAM
10 MB freier Speicherplatz auf der Festplatte
Super VGA (800 x 600)

Windows 7, Vista, 2008
1-GHz-Prozessor, 32 Bit (x86) / 64 Bit (x64)
512 MB RAM
10 MB freier Speicherplatz auf der Festplatte
Super VGA (800 x 600)

12.7 Häufige Fragen (FAQ)

Muss ESET SysInspector mit Administratorrechten ausgeführt werden?

ESET SysInspector muss zwar nicht unbedingt mit Administratorrechten ausgeführt werden, einige Informationen können jedoch nur über ein Administratorkonto erfasst werden. Bei einer Ausführung unter einer niedrigeren Berechtigungsstufe (Standardbenutzer, eingeschränkter Benutzer) werden daher weniger Informationen zur Systemumgebung erfasst.

Erstellt ESET SysInspector eine Log-Datei?

ESET SysInspector kann eine Log-Datei mit der Konfiguration Ihres Computers erstellen. Hierzu klicken Sie im Hauptmenü auf Datei > Log speichern. Die Logs werden im XML-Format gespeichert. Standardmäßig erfolgt dies im Verzeichnis %USERPROFILE%\Eigene Dateien\ und unter einem Namen nach dem Muster „SysInspector-%COMPUTERNAME%-JJMMTT-HHMM.XML“. Speicherort und Name der Log-Datei können Sie beim Speichern natürlich noch ändern.

Wie zeige ich eine ESET SysInspector-Log-Datei an?

Um eine von ESET SysInspector erstellte Log-Datei anzuzeigen, starten Sie das Programm und klicken im Hauptmenü auf Datei > Log öffnen. Sie können Log-Dateien auch auf ESET SysInspector ziehen und dort ablegen. Wenn Sie häufig Log-Dateien aus ESET SysInspector anzeigen müssen, empfiehlt es sich, auf dem Desktop eine Verknüpfung zur Datei SYSINSPECTOR.EXE anzulegen. So können Sie Log-Dateien einfach auf dieses Symbol ziehen, um sie zu öffnen. Aus Sicherheitsgründen lässt Windows Vista unter Umständen kein Drag&Drop zwischen Fenstern mit unterschiedlichen Berechtigungsstufen zu.

Ist das Format der Log-Datei dokumentiert? Gibt es ein SDK?

Da sich das Programm noch in der Entwicklung befindet, gibt es momentan weder eine Dokumentation für das Dateiformat noch ein SDK. Je nach Kundennachfrage wird sich dies nach der offiziellen Veröffentlichung des Programms eventuell ändern.

Wie bewertet ESET SysInspector das Risiko, das von einem bestimmten Objekt ausgeht?

Um Objekten wie Dateien, Prozessen, Registrierungsschlüsseln usw. eine Risikostufe zuzuordnen, verwendet ESET SysInspector in der Regel einen Satz heuristischer Regeln, mit denen die Merkmale des Objekts untersucht werden, um anschließend nach entsprechender Gewichtung das Potenzial für schädliche Aktivitäten abschätzen. Auf der Grundlage dieser Heuristik wird den Objekten so eine Risikostufe von „1 - In Ordnung" (grün) bis „9 - Risikoreich" (rot) zugeordnet. Die Farbe der Abschnitte im Navigationsbereich im linken Teil des Programmfensters richtet sich nach der höchsten Risikostufe, die ein darin enthaltenes Objekt hat.

Bedeutet die Risikostufe „6 - Unbekannt" (rot), dass eine Gefahr vom betreffenden Objekt ausgeht?

Die Einschätzung von ESET SysInspector legt nicht endgültig fest, ob eine Gefahr von einem Objekt ausgeht. Diese Entscheidung muss ein Sicherheitsexperte treffen. ESET SysInspector kann hierbei helfen, indem es dem Experten schnell zeigt, welche Objekte eventuell gründlicher untersucht werden müssen.

Warum stellt ESET SysInspector beim Start eine Verbindung ins Internet her?

Wie viele Anwendungen ist auch ESET SysInspector mit einem digitalen Zertifikat signiert, mit dem überprüft werden kann, dass die Software tatsächlich von ESET stammt und nicht verändert wurde. Hierzu baut das Betriebssystem eine Verbindung zu einer Zertifizierungsstelle auf, um die Identität des Softwareherstellers zu überprüfen. Es handelt sich dabei um einen normalen Vorgang, den alle digital signierten Programme unter Microsoft Windows ausführen.

Was ist Anti-Stealth-Technologie?

Die Anti-Stealth-Technologie ermöglicht eine effektive Erkennung von Rootkits.
Wenn ein System von einem Schadprogramm angegriffen wird, das sich als Rootkit in das System einbindet, besteht ein hohes Risiko, dass Daten unbemerkt beschädigt, gelöscht oder gestohlen werden. Ohne spezielle Tools ist es quasi unmöglich, solche Rootkits zu erkennen.

Warum ist bei Dateien manchmal Microsoft als Unterzeichner angegeben, wenn gleichzeitig aber ein anderer Firmenname angezeigt wird?

Wenn SysInspector versucht, die digitale Signatur einer Programmdatei zu überprüfen, wird zunächst nach einer eingebetteten digitalen Signatur in der Datei gesucht. Wenn eine solche vorhanden ist, werden die darin enthaltenen Informationen zur Überprüfung verwendet. Falls die Datei hingegen keine digitale Signatur enthält, sucht SysInspector nach einer passenden CAT-Datei (im Sicherheitskatalog - %systemroot%\system32\catroot) mit Informationen zu der betreffenden Programmdatei. Ist diese Suche erfolgreich, wird die digitale Signatur dieser CAT-Datei zur Überprüfung der Programmdatei verwendet.

In einem solchen Fall kann es dann dazu kommen, dass Microsoft als Unterzeichner angegeben ist, die Angabe „Firmenname" jedoch davon abweicht.

Beispiel:

Windows 2000 enthält die Anwendung „HyperTerminal" in *C:\Programme\Windows NT*. Die Haupt-Programmdatei dieser Anwendung ist nicht digital signiert. SysInspector weist jedoch Microsoft als Unterzeichner aus. Dies liegt daran, dass in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* ein Verweis auf *C:\Programme\Windows NT\hypertrm.exe* (die Haupt-Programmdatei von HyperTerminal) vorhanden ist und *sp4.cat* wiederum durch Microsoft digital signiert wurde.

13. ESET SysRescue

ESET SysRescue ist ein Utility, mit dem Sie einen bootfähigen Datenträger mit ESET NOD32 Antivirus (EAV) oder ESET Smart Security (ESS) erstellen können. Der große Vorteil von ESET SysRescue ist, dass ESS bzw. EAV damit unabhängig vom Betriebssystem auf dem jeweiligen Rechner ausgeführt werden kann und direkten Zugriff auf die Festplatte sowie das gesamte Dateisystem hat. Auf diese Weise lassen sich auch Infektionen entfernen, bei denen dies normalerweise (bei laufendem Betriebssystem usw.) nicht möglich wäre.

13.1 Minimalanforderungen

ESET SysRescue verwendet das Microsoft Windows Preinstallation Environment (Windows PE) Version 2.x, das wiederum auf Windows Vista basiert. Windows PE ist Teil des kostenlosen Windows Automated Installation Kit (Windows AIK). Vor dem Erstellen einer ESET SysRescue-CD muss daher das Windows AIK in der Version 936330AIK installiert werden (http://www.microsoft.com/Downloads/details.aspx?familyid=94BB6E34-D890-4932-81A5-5B50C657DE08&displaylang=en). Da die 32-Bit-Version von Windows PE unterstützt wird, muss beim Erstellen von ESET SysRescue auf 64-Bit-Systemen ein 32-Bit-Installationspaket von ESS/EAV verwendet werden. ESET SysRescue unterstützt Windows AIK 1.1 und höher und ist in ESS/EAV ab der Version 4.0 verfügbar.

Unterstützte Betriebssysteme:

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Server 2008
- Windows Server 2003 Service Pack 1 mit KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 mit KB926044

13.2 Erstellen der Rettungs-CD

Wenn die Minimalanforderungen für die Erstellung der ESET SysRescue-CD erfüllt sind, sollte es keine Probleme geben. Klicken Sie auf **Start** > **Programme** > **ESET** > **ESET NOD32 Antivirus** > **ESET SysRescue**, um den ESET SysRescue-Assistenten zu starten.

Zuerst prüft der Assistent, ob Windows AIK und ein geeignetes Gerät für die Erstellung des Bootmediums verfügbar sind.

Im nächsten Schritt wählen Sie das Zielmedium für ESET SysRescue aus. Neben CD/DVD/USB können Sie ESET SysRescue auch in einer ISO-Datei speichern. Später können Sie dann das ISO-Abbild auf CD/DVD brennen oder es anderweitig verwenden (z. B. in einer virtuellen Umgebung wie VMware oder VirtualBox).

Nachdem Sie alle Einstellungen vorgenommen haben, sehen Sie im letzten Schritt des ESET SysRescue-Assistenten eine Kompilierungsvorschau. Prüfen Sie die Einstellungen und starten Sie die Kompilierung. Es stehen die folgenden Optionen zur Verfügung:

Ordner 112
ESET Antivirus 112
Erweitert 112
Bootfähiges USB-Gerät 112
Brennen 113

13.2.1 Ordner

Temporärer Ordner ist das Arbeitsverzeichnis für die bei der Kompilierung eines ESET SysRescue-Mediums erforderlichen Dateien.

ISO-Ordner ist der Ordner, in dem die fertige ISO-Datei nach Abschluss der Kompilierung gespeichert wird.

In der Liste auf dieser Registerkarte werden alle lokalen und verbundenen Netzlaufwerke mit dem jeweils verfügbaren freien Speicherplatz angezeigt. Falls einer der hier angegebenen Ordner auf einem Laufwerk mit zu wenig freiem Speicherplatz liegt, sollten Sie ein anderes Laufwerk mit mehr freiem Speicherplatz auswählen. Anderenfalls bricht die Kompilierung möglicherweise vorzeitig ab.

13.2.2 ESET Antivirus

Beim Erstellen einer ESET SysRescue-CD können Sie zwei Quellen für die vom Compiler zu verwendenden ESET-Dateien wählen.

ESS/EAV-Ordner - Es werden die bereits vorhandenen Dateien aus dem Ordner verwendet, in dem das ESET Produkt auf dem Computer installiert ist.
MSI-Datei - Es werden die im MSI-Installationspaket enthaltenen Dateien verwendet.
Profil - Hier legen Sie fest, welcher Quelle der Benutzername und das Passwort für Updates entnommen werden:
ESS/EAV-Installation - Benutzername und Passwort werden der vorhandenen Installation von ESET Smart Security bzw. ESET NOD32 Antivirus entnommen
Von Benutzer - Es werden der Benutzername und das Passwort verwendet, die Sie in den dazugehörigen Feldern eingeben.

HINWEIS: ESET Smart Security bzw. ESET NOD32 Antivirus auf der ESET SysRescue-CD werden entweder über das Internet oder über die ESET Security-Lösung aktualisiert, die auf dem Computer installiert ist, auf dem die ESET SysRescue-CD ausgeführt wird.

13.2.3 Erweiterte Einstellungen

Auf der Registerkarte **Erweitert** können Sie die ESET SysRescue-CD für die Größe des Arbeitsspeichers auf Ihrem Computer optimieren. Wenn Sie **512 MB oder mehr** wählen, wird der Inhalt der CD in den Arbeitsspeicher (RAM) geschrieben. Bei der Einstellung **weniger als 512 MB** findet im Betrieb von WinPE hingegen laufend ein Zugriff auf die Rettungs-CD statt.

Externe Treiber - In diesem Bereich können Sie Treiber für Ihre Hardware (z. B. Netzwerkadapter) hinzufügen. Da WinPE auf Windows Vista SP1 basiert, ist eine breite Hardwareunterstützung gegeben. In manchen Fällen kann es jedoch vorkommen, dass Hardware nicht erkannt wird und Sie den Treiber von Hand hinzufügen müssen. Um den Treiber in ESET SysRescue zu integrieren, gibt es zwei Möglichkeiten: manuell (über die Schaltfläche **Hinzufügen**) oder automatisch (Schaltfläche **Autom. Suche**). Bei der manuellen Methode müssen Sie den Pfad zur passenden .inf-Datei auswählen (die dazugehörige .sys-Datei muss ebenfalls in diesem Ordner liegen). Bei der automatischen Methode wird der Treiber automatisch im Betriebssystem des aktuellen Computers gesucht. Diese Methode sollten Sie nur verwenden, wenn Sie ESET SysRescue später auf einem Computer mit derselben Hardware (z. B. Netzwerkadapter) wie dem Computer nutzen, auf dem Sie die ESET SysRescue-CD erstellt haben. Bei der Erstellung der ESET SysRescue-CD wird der Treiber dann integriert, sodass Sie ihn später nicht mehr separat suchen müssen.

13.2.4 Bootfähiges USB-Gerät

Falls Sie ein USB-Gerät als Zielmedium ausgewählt haben, können Sie eines der verfügbaren USB-Medien auf der Registerkarte **Bootfähiges USB-Gerät** auswählen (falls mehrere USB-Geräte vorhanden sind).

13.2.5 Brennen

Wenn Sie CD/DVD als Zielmedium ausgewählt haben, können Sie weitere Parameter für das Brennen auf der Registerkarte „Brennen" festlegen.

ISO-Datei löschen - Aktivieren Sie diese Option, um die ISO-Datei nach dem Erstellen der ESET SysRescue-CD zu löschen.
Löschen aktiviert - Sie können zwischen schnellem Löschen und vollständigem Löschen auswählen.
Brennerlaufwerk - Wählen Sie das Laufwerk zum Brennen aus.

Warnung: Dies ist die Standardoption. Falls Sie eine wiederbeschreibbare CD/DVD verwenden, werden alle zuvor darauf gespeicherten Daten gelöscht.

Der Bereich „Medium" enthält Informationen über das aktuell in Ihrem CD/DVD-Laufwerk eingelegte Medium.

Schreibgeschwindigkeit - Wählen Sie die gewünschte Geschwindigkeit in der Liste aus. Berücksichtigen Sie dabei die Fähigkeiten Ihres Brenners und den Typ des CD-/DVD-Rohlings.

13.3 Die Arbeit mit ESET SysRescue

Damit die Rettungs-CD (bzw. DVD/USB) wie erwartet funktioniert, müssen Sie Ihren Computer vom ESET SysRescue-Bootmedium starten. Die Bootreihenfolge können Sie ggf. im BIOS entsprechend abändern. Alternativ können Sie auch beim Start des Computers das Bootmenü aufrufen. Je nach Motherboard und BIOS geschieht dies meist über eine der Tasten F9 bis F12.

Nach dem Hochfahren startet ESS bzw. EAV. Da ESET SysRescue nur in bestimmten Situationen verwendet wird, sind einige Schutzkomponenten und Programmfunktionen aus dem normalen Betrieb von ESS/EAV entbehrlich. Es werden daher nur die Komponenten **Computer prüfen**, **Update** sowie einige Bereiche unter **Einstellungen** geladen. Für den erfolgreichen Einsatz von ESET SysRescue ist insbesondere eine aktuelle Signaturdatenbank sehr wichtig. Vor einer Prüfung des Computers sollten Sie daher zunächst ein Programm-Update starten.

13.3.1 Verwenden des ESET SysRescue-Mediums

Nehmen wir an, dass Computer im Netzwerk mit einem Virus infiziert wurden, der ausführbare Dateien (EXE) befällt. Mit ESS/ENA können Sie alle infizierten Dateien bereinigen. Einzige Ausnahme ist die Datei explorer.exe, die selbst im abgesicherten Modus nicht gesäubert werden kann.
Dies liegt daran, dass explorer.exe als einer der grundlegenden Windows-Prozesse auch im abgesicherten Modus gestartet wird. ESS/EAV kann mit der Datei keine Aktionen ausführen, sodass sie infiziert bleibt.
In diesem Fall können Sie das Problem mit ESET SysRescue beheben, da ESET SysRescue keine Komponenten des Host-Betriebssystems benötigt. Deshalb kann es alle Dateien auf der Festplatte verarbeiten (säubern oder löschen).